Privacy Advocates

Альманах ПД

Комплаенс ПД и информационная приватность в РФ

- Редакция от 25 октября 2026 года
- privacy-advocates.ru/pd

Четыре уровня Альманаха и три пути к любому слайду

Читается подряд как пособие, по карте как справочник, по чек-листу как программа комплаенса

Privacy Advocates

ЧЕТЫРЕ УРОВНЯ

10 частей — **Часть**
I-X, от рамки регулирования до тайн и защиты информации

37 разделов — **Раздел**
01-37, бывшие презентации и новые темы

133 подразделов — **Подраздел**
например 20.1-20.5, разделы презентаций

720 слайдов — **Слайд**
постоянный ID вида TPD-006

ТРИ ПУТИ

Карта Альманаха

Все 37 разделов на одном слайде. Клик по разделу открывает его обложку, по части ее разделитель

Навигатор по чек-листу ПД

10 разделов чек-листа и разделы Альманаха, где раскрыты их контроли

Навигационная строка

Внизу каждого слайда часть, раздел, подраздел и ID слайда, значок слева возвращает к карте

Часть V | 20 ТПД | 20.1 Понятие и регулирование | **TPD-006**

Оговорка. Материал отражает регулирование на дату редакции и не является юридической консультацией. Ссылки внутри PDF работают в любом просмотрщике.

Десять частей ведут от рамки к отраслевым разборам

Клик по разделу открывает его обложку, по номеру части ее разделитель

Privacy Advocates

I Ландшафт и ценности

- 01 Тренды
- 02 Этика данных

II Фундамент комплаенса

- 03 Обзор комплаенса
- 04 Осведомленность
- 05 Определение ПД
- 06 Допустимость

III DPO и организация

- 07 Организация
- 08 Профессия
- 09 Автоматизация

IV Основания и категории

- 10 Основания
- 11 ПД работников
- 12 ПД потребителей
- 13 Маркетинг
- 14 Распространение
- 15 Биометрия
- 16 Генетика
- 17 Права субъектов

V Хранение и передачи

- 18 Уничтожение ПД
- 19 Локализация
- 20 ТПД
- 21 Поручение и DTA

VI Цифровая среда и ИИ

- 22 Сайт
- 23 Авторизация
- 24 ИИ и ПД
- 25 Дипфейки

VII Риски и инциденты

- 26 Прайваси-риски
- 27 Защита и СЗПД
- 28 Инциденты

VIII Надзор и ответственность

- 29 РКН и органы
- 30 Ответственность
- 31 Практика КоАП
- 32 Резонансные дела

IX Отраслевые разборы

- 33 Адвокаты
- 34 Банкротство
- 35 Фармаконадзор

X Тайны и защита

- 36 Защита информации
- 37 Коммерческая тайна

ФИНАЛ | Ресурсы и контакты | Материалы для скачивания | Юмор Альманаха

Каждый раздел чек-листа ведет к своим разделам Альманаха

Чек-лист основных контролей обработки и защиты ПД, редакция 2026.10.19: 10 разделов и 132 контроля

Privacy Advocates

РАЗДЕЛ ЧЕК-ЛИСТА	КРИТИЧНОСТЬ	РАЗДЕЛЫ АЛЬМАНАХА
1 Руководство и учет	**10** контролей	**07** Организация · **08** Профессия · **09** Автоматизация
2 Целенаправленность и пропорциональность	**9** контролей	**06** Допустимость · **05** Определение ПД · **12** ПД потребителей
3 Основания обработки	**26** контролей	**10** Основания · **11** ПД работников · **14** Распространение
4 Сбор, хранение и уничтожение	**17** контролей	**18** Уничтожение ПД · **19** Локализация · **23** Авторизация · **22** Сайт
5 Передача и соглашения с третьими лицами	**15** контролей	**21** Поручение и DTA · **20** ТПД · **14** Распространение · **24** ИИ и ПД
6 Коммуникация с субъектами	**18** контролей	**17** Права субъектов · **22** Сайт · **14** Распространение · **13** Маркетинг
7 Взаимодействие с органами	**11** контролей	**29** РКН и органы · **20** ТПД · **19** Локализация · **22** Сайт
8 Осведомленность персонала	**4** контроля	**04** Осведомленность · **07** Организация
9 Безопасность обработки	**15** контролей	**27** Защита и СЗПД · **26** Прайваси-риски · **18** Уничтожение ПД
10 Отклонения и инциденты	**7** контролей	**28** Инциденты · **07** Организация
Приложение 1. Меры ответственности		**30** Ответственность · **31** Практика КоАП · **32** Резонансные дела
Приложение 2. Риск-факторы надзора		**29** РКН и органы · **01** Тренды

Давайте знакомиться

Кто говорит и почему его стоит послушать

Privacy Advocates



Алексей Мунтян

Управляющий партнер
Privacy Advocates

+7 (903) 762-64-15

alexey.muntyan@
privacy-advocates.ru

- 18 лет опыта в комплаенсе персональных данных и информационной приватности
- Соучредитель "Сообщества профессионалов в области инфоприватности" - RPPA.pro
- Участник центра компетенций Роскомнадзора и научно-технического совета ГРЧЦ
- Член государственной экзаменационной комиссии Высшей школы права РЭУ им. Г.В. Плеханова
- Сопредседатель Privacy & Legal Innovation кластера РАЭК
- Ex-DPO в Johnson&Johnson, DHL Express, "Альфа-Групп", Sber CIB и Восточно-африканском офисе Управления Верховного комиссара ООН по правам человека

ЧАСТЬ

I

Ландшафт и ценности

Куда движется регулирование и на каких ценностях держится приватность

01 Тренды регулирования ПД

02 Этика и культура данных

01

Тренды регулирования ПД

Ретроспектива 2025 и перспективы 2026-2028: что важно знать оператору ПД

01.1 Ретроспектива 2025-2026

01.2 Перспективы 2026-2028

01.3 Антифрод-3

Раздел на сайте
privacy-advocates.ru/pd/tre

01.1

Ретроспектива 2025-2026

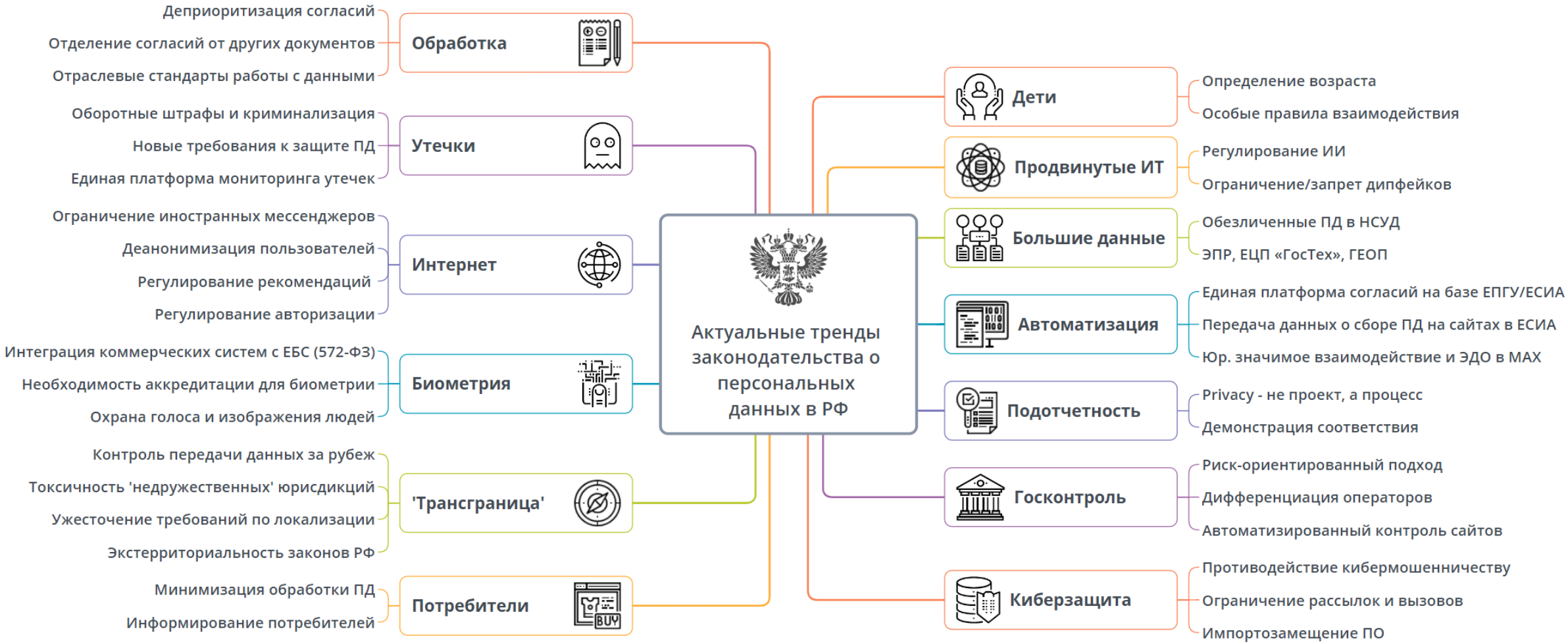
Что уже стало законом, как изменился контроль и чему научила судебная практика

- Тренды законодательства о ПД в РФ
- Основные регуляторные новеллы 2020-2024
- Основные регуляторные новеллы 2025-2026
- Усиление ответственности за ПД

Тренды законодательства о ПД в РФ

Обработка, ответственность, приземление, приватность, интернет, ТПД, потребители

Privacy Advocates



Основные регуляторные новеллы 2020-2024

Четыре линии реформы на одной карте

Privacy Advocates

	2020	2022	2023	2024
Ответственность		**260-ФЗ** сбор ПД иностранцами	**277-ФЗ** иностранные мессенджеры	**78-ФЗ** спам-звонки, ст.14.3 КоАП **420-ФЗ** оборотные штрафы за утечки **421-ФЗ** ст.272.1 УК, оборот ПД
Обработка	**519-ФЗ** распространение ПД	**266-ФЗ** реформа 152-ФЗ		**158-ФЗ** право на забвение **233-ФЗ** обезличивание и НСУД
Идентификация и биометрия		**572-ФЗ** биометрия и ЕБС	**406-ФЗ** авторизация на сайтах **408-ФЗ рекомендательные технологии** **589-ФЗ** штрафы за биометрию	
Контроль и надзор				**540-ФЗ** реформа контроля, ПП № 1046

Основные регуляторные новеллы 2025-2026

Эра антифрода, приземления и искусственного интеллекта

Privacy Advocates

	2025		2026	
Ответственность	104-ФЗ	штрафы по ст.13.12 КоАП	199-ФЗ	ст.13.55 и 13.56 КоАП
	281-ФЗ	ст.13.29.2 и 19.5.3 КоАП		
	508-ФЗ	дела 13.11 снова в общих судах		
Антифрод	41-ФЗ	Антифрод-1	210-ФЗ	Антифрод-2
	156-ФЗ	обособление согласий		
Локализация и трансграничная передача	23-ФЗ	локализация 2.0, ПД силовиков	43-ФЗ	генетические данные
	140-ФЗ	ПД клиентов экспедиторов	265-ФЗ	новый критерий перечня адекватных стран
	351-ФЗ	исследования и опросы		
Госдоступ и ИИ	244-ФЗ	регулирование ЦОД	52-ФЗ	геномная регистрация
	492-ФЗ	копии баз данных для ФСБ	55-ФЗ	справки МВД об адресах
			130-ФЗ	ИИ-образы в агитации
			243-ФЗ	поддержка ИИ

Усиление ответственности за ПД

Пакет законов 2024-2025 и его первые итоги

Privacy Advocates

3-20 млн ₽

Ст.13.11 КоАП РФ: утечки

или 1-3% годового оборота за повторную утечку, 1-3 млн ₽ за неуведомление РКН; статья расширена до восемнадцати частей (420-ФЗ).

923 случая

Ст.272.1 УК РФ

за 10 месяцев 2025 г., в основном против пробивщиков и инсайдеров; топ-менеджеров за утечки пока судят по ст.274 УК РФ (Сирена-трэвел, новое рассмотрение).

до 100 тыс. ₽

Ст.13.12 КоАП РФ

за нарушение требований о защите информации, при несертифицированных СЗИ с конфискацией (104-ФЗ от 23.05.2025).

01.01.2026

Возврат дел в СОЮ

все дела по ст.13.11 КоАП РФ вновь рассматривают суды общей юрисдикции (508-ФЗ); арбитражные суды разбирали дела о ПД лишь с 30.05.2025.

План 2207-р, п.4: к III кварталу 2027 г. МВД, Минцифры, Минэкономразвития, ФСБ и РКН представят предложения о дальнейшем повышении ответственности и увеличении срока давности по нарушениям в области ПД.

Локализация баз с ПД 2.0 с 01.07.2025

Уточненные требования 23-ФЗ и волна штрафов 2026 года

Privacy Advocates

01

Концепция локализации

Основная концепция при сборе ПД не затронута, но переформулирована: запрет вести операции записи, накопления и хранения в зарубежных базах.

02

Момент завершения сбора

Аргументированное и доказуемое определение момента завершения сбора ПД и окончания применимости ч.5 ст.18 152-ФЗ становится критичным.

03

Зарубежные базы

Не размещать собранные в РФ ПД в контролируемых зарубежных БД и не признавать использование таких БД в обработке собранных ПД.

Практика 2026: иностранные игроки

Не менее 7 исков РКН к зарубежным игровым компаниям (EA, Take-Two, NetEase, Battlestate Games, Embracer - по 1-2 млн ₽), штрафы Duolingo и Miro (по 2 млн ₽), Change.org (1 млн ₽), SSI International (6 млн ₽ за повтор).

ПЕРСОНАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

На Кубани должностное лицо администрации района оштрафовано на 100 тыс. ₽ за иностранную платформу в коде сайта; банки и МФО получили не менее 21 дела по ст.13.11.2 КоАП РФ за переписку с клиентами в WhatsApp.

Новые правила обезличивания ПД с 01.09.2025

Обезличенные ПД остаются ПД, а требования Минцифры о передаче в НСУД уже работают

Privacy Advocates

Это тоже ПД

Обезличивание - действия, после которых невозможно без дополнительной информации определить принадлежность ПД субъекту (п.9 ст.3 152-ФЗ).

Не способ уничтожения

По достижении целей ч.4 ст.21 требует уничтожения, а ч.7 ст.5 допускает и обезличивание.

Особые требования

К процессу и методам обезличивания применяются требования и методы, утвержденные приказом РКН.

Требование о передаче в НСУД

С 01.09.2025 (ст.13.1 152-ФЗ) операторам может поступить требование обезличить ПД и передать их в ГИС ЕИП НСУД.

ПРИКАЗ МИНЦИФРЫ ОТ 03.03.2026 № 173

Утверждены методические рекомендации по подготовке требований об обезличивании; проект ПП РФ (07.05.2026) допускает передачу статистических показателей без специального ПО и СМЭВ, бизнес (АБД) просит отсрочку до 2027 г.

Инициатива АБД, 03.08.2026

Разрешить обработку ПД с применением технологий приватности (PETs) без согласия субъектов для обучения моделей ИИ.

Обособление согласия на обработку ПД с 01.09.2025

Ч.1 ст.9 152-ФЗ: согласие оформляют отдельно от иных информации и документов - как трактовать?

Privacy Advocates

01

Визуальное и смысловое отделение

Согласие отделено от других документов: пользовательское соглашение - отдельно, согласие - отдельно.

02

Отдельное волеизъявление

Предоставление согласия отдельным действием: например, отдельная галочка, а не подпись под общим документом.

03

Утвержденные формы

Формы, утвержденные актами органов власти (например, по ЕБС), обязательны к исполнению (РКН устно 22.08.2025, 14.08.2026).

ВС РФ, 22.06.2026

Встречное согласие на рекламу за скидку правомерно

Дело Мэлон Фэшн Груп: согласие на рекламу в обмен на скидку является надлежащим, продавец не обязан давать скидку без согласия.

ПРОЕКТ ПРОВЕРОЧНОГО ЛИСТА РКН, 03.08.2026

77 вопросов вместо 75

5 новых вопросов: критерии и обособление согласия, уничтожение по достижении целей, уведомление по каждой цели. Исключены 3, среди них вопрос 33 об оргмерах. В начале октября 2026 года еще проект.

Контроль за обработкой ПД в 2026 году

Новая редакция ПП РФ № 1046 (с 02.09.2025)

План профвизитов 2026
скачать

Privacy Advocates

Высокий

проверка раз в 2 года или ежегодный профвизит

Значительный

обязательный профвизит не чаще раза в 3 года

Средний

обязательный профвизит не чаще раза в 5 лет

Умеренный

обязательный профвизит не чаще раза в 6 лет

Низкий

плановых мероприятий и профвизитов нет

Группа тяжести А теперь включает обработку ПД на основании согласия, если закон не требует его получения; группы вероятности синхронизированы со ст.13.11, 13.11.2, 13.11.3 КоАП РФ.

План профвизитов на 2026 (приказ РКН от 19.12.2025 № 390): 1156 операторов, включая госучреждения, школы и медцентры; свою категорию риска можно проверить в Едином реестре видов контроля.

Дистанционный контроль: по итогам мероприятия без взаимодействия оператору могут направить не только предостережение, но и требование об уничтожении ПД.

Автоматизированный дистанционный контроль

АС МПД: как устроен мониторинг сайтов и что он выявляет

Privacy Advocates

89%

точность автоматического выявления признаков нарушений

500 тыс.

ресурсов в год по ТЗ (фактически около 50 тыс.), не менее 15 тыс. в неделю

77% / 84%

ресурсов с признаками нарушений в 2024 г. и за полгода 2025 г.

8 тыс.

требований о приведении сайтов в соответствие за полгода 2025 г. (6,5 тыс. за 2024 г.)

ЧТО ИЩЕТ СИСТЕМА

- нет согласия на обработку ПД, нет политики, объем формы шире политики
- ссылки на сторонние формы сбора, сбор ПД россиян при зарубежном хостинге
- нет информации о трансграничной передаче, метрические программы без указания в политике
- некорректный срок прекращения обработки, обработка без уведомления РКН

Кого проверяют в первую очередь

Финансово-кредитные организации, страховщики, коллекторы, соцсети, операторы связи, интернет-магазины, перевозчики, почтовые сервисы, медицинские и образовательные учреждения, ЖКХ и управляющие компании, МФЦ, органы власти - сферы с наибольшим числом жалоб граждан.

Судебная практика 2025 по ст.13.11 КоАП РФ

Смешение практики СОЮ (до 30 мая) и арбитражных судов (с 30 мая)

Privacy Advocates

Распределение дел по составам ст.13.11 КоАП



Кого привлекали: банки, телеком, госучреждения, школы, больницы, цифровые сервисы, ЖКУ (УК, ТСЖ, СНТ), физлица.

Более 57% дел закончились предупреждением (первое привлечение, признание вины, устранение нарушений); инициаторы - Роскомнадзор (72%) и прокуратура (28%).

Ориентиры года: ФИО и адрес автора отзыва могут не быть ПД, а посредник не отвечает за чужой контент, пока не узнал о нарушении (АС Москвы, 07.11.2025); передача ПД работника подрядчику по бухучету и арендодателю для пропуска согласия не требует (Савеловский райсуд, 02.07.2025).

Крупных штрафов по новым спецсоставам ст.13.11 КоАП РФ в 2025 году не отмечено.

Судебная практика 2026 по ст.13.11 КоАП РФ

Акты 2026 года на 14.10.2026

Privacy Advocates

244

актов: 73 мировых судей, 83 арбитражных суда, 29 пересмотров в райсудах, 59 проверочных инстанций

77 / 44

штрафов и предупреждений в первой инстанции: у мировых судей предупреждений три, в арбитраже - 41 из 64

150 тыс. ₽

медианный штраф по ч.1 у мировых судей; в арбитражных судах медиана 75 тыс. ₽

6 млн ₽

восемь штрафов иностранным операторам за повторную нелокализацию (ч.9)

Распределение актов по составам ст.13.11 КоАП



Кого привлекают: иностранные операторы (30 актов, дайвинг-ассоциации PADI, NAUI, SNSI, AIDA), ЖКХ (30), телеком (26), госсектор (18), утечки (17), банки (14), школы (11), клиники, коллекторы, страховщики.

Инициатор: Роскомнадзор в 234 актах, прокуратура в 7 актах, а в 3 оставшихся инициатор в тексте не назван либо спор частный.

Пересмотр: 88 актов райсудов, апелляций и кассаций: 60 оставлены без изменения, 10 направлены на новое рассмотрение, 15 отменены полностью или в части (6 с прекращением), 3 иных исхода.

Сдвиг года: два трека санкции: мировые судьи почти всегда штрафуют (три предупреждения в Санкт-Петербурге в мае и одно освобождение по малозначительности, ст.2.9 КоАП, в Москве в июне 2026), арбитражные суды заменяют штраф предупреждением в двух делах из трех; крупные суммы дает только нелокализация.

Судебная практика 2026: утечка не равна вине оператора

Объективное вменение отступает, но подрядчик и молчание не спасают

Privacy Advocates

ДЕЛО РЖД - АС МО, 10.06.2026

Сам факт утечки не означает вину оператора

РКН обязан доказать, какие меры оператор мог принять, но не принял; сам факт атаки и уголовное дело по ст.272.1 УК РФ недостаточность мер не доказывают.

МИНТРУД И РОСТЕЛЕКОМ - 2026

Подрядчик не снимает ответственности с оператора

ВС РФ 21.01.2026 учел против оператора неуведомление РКН и отсутствие внутреннего контроля. АС СЗО 02.10.2026 по делу Ростелекома указал, что оператор отвечает за подрядчика (ч.5 ст.6), утечка длящееся нарушение, а отказ устоял лишь из-за давности.

ОРИОН ТЕЛЕКОМ И ТД АСК - 2025-2026

Замена на предупреждение не гарантирована

Самоуведомление РКН, МСП и первичность помогали, но 4 ААС (11.08.2026) счел замену по ч.13 необоснованной и сохранил ее лишь из-за давности. Отчет о расследовании бьет по оператору.

ЛОКАЛИЗАЦИЯ - 2026

Волна исков к иностранным компаниям

Игровые компании, Taobao (1 млн ₽, апелляция 29.09.2026), Duolingo, Change.org, Miro и SSI International; оштрафовано должностное лицо администрации района за иностранную платформу в коде сайта.

01.2

Перспективы 2026-2028

Согласие уходит с трона, стандарты и приземление приходят на смену, данные переходят из слабых рук в сильные

- Симптомы исчерпания концепции согласия
- Утилизация "культа согласий"
- Регуляторная деприоритезация согласий
- Платформа согласий в Антифрод-3

Симптомы исчерпания концепции согласия

Каждая реформа добавляла согласию новое обязательное свойство

Privacy Advocates

2007

Решение о даче согласия

Собственная воля, собственный интерес, свободно

2011

Выражение согласия

Конкретное, информированное, сознательное

2022

Выражение согласия

Предметное, однозначное

2025

Оформление согласия

Обособленное - отдельно от иных документов (156-ФЗ)

Итог: чем больше признаков должно сойтись в одном документе, тем выше потенциал его оспоримости и тем дороже его администрирование - регулятор сам называет институт морально устаревшим.

Утилизация "культа согласий"

Позиция Роскомнадзора: институт согласия устарел, нужны отраслевые стандарты

Privacy Advocates

Институт согласия на обработку персональных данных является морально устаревшим… Необходим переход от текущей модели к внедрению отраслевых стандартов…

Руководитель Роскомнадзора Андрей Липов, 31.10.2025

ЗАМЕСТИТЕЛЬ РУКОВОДИТЕЛЯ РКН МИЛОШ ВАГНЕР, 30.06.2025

1. согласие стоит первым среди равновеликих оснований и, по всей видимости, ошибочно воспринимается как главное
2. взять его легко, правовых и административных рисков для компании оно не несет, а при отзыве компания без труда подбирает другое основание

Регуляторная деприоритезация согласий

Платформа согласий на базе ЕСИА: от антифрод-пакетов к Доктрине

Privacy Advocates

06.2026

не вошло в закон

Антифрод-2 (210-ФЗ)

Согласия через ЕСИА, обжалование через ЕПГУ и реестр всех согласий обсуждались, но в итоговую редакцию не попали.

30.09.2026

возвращено в проект

Антифрод-3

Согласие и отзыв через ЕСИА, сведения обо всех согласиях в ЕСИА, просмотр и жалоба через ЕПГУ; в редакции 19.08.2026 блок исключался.

22.07.2026

закреплено в проекте

Доктрина ИКТ

Платформа согласий на базе ЕСИА, сокращение случаев обработки по согласию, идентификация без передачи ПД. Основа до 2030 г., внедрение в 2030-2035 гг.

2026

инициативы депутатов

Отзыв согласий

Единый сервис отзыва на Госуслугах (01.04.2026) и отзыв в той же форме, в которой согласие получено (21.02.2026).

Издержки и риски деприоритезации: повышение стандартов получения/отзыва согласий и увеличение потенциала оспоримости согласий (ч.1 ст.9 152-ФЗ); согласие вне обязанности по закону - группа тяжести А (ПП-1046), а по Антифрод 3.0 требовать его запрещено (ч.2.1 ст.18); стоимость интеграции учета согласий с ЕСИА/ЕПГУ

Платформа согласий в Антифрод-3

Проект от 30.09.2026: согласия, отзывы и жалобы получают канал через ЕСИА и ЕПГУ

Privacy Advocates

Правительство РФ: случаи, порядок и состав сведений

Субъект ПД

дает и отзывает согласие через ЕСИА **ч.1.1, 2.1 ст.9**

видит на ЕПГУ, кто обрабатывает его ПД по согласию **ч.7.1 ст.14**

ЕСИА
ЕПГУ

сообщает в ЕСИА о согласиях и отзывах, полученных напрямую **ч.1.2, 2.2 ст.9**

не вправе требовать согласие сверх закона и отраслевых актов **ч.2.1 ст.18**

Оператор ПД

Роскомнадзор: жалобы через ЕПГУ (ч.1.1 ст.17), типовые формы согласий вместе с Минцифры (ч.1.3 ст.9)

Что меняется для оператора: согласия и отзывы учитываются в двух каналах, а сведения о полученных напрямую передаются в ЕСИА. Согласие на распространение - только непосредственно оператору, канал через ИС РКН упраздняется (ст.10.1). На финрынке порядок согласуется с Банком России, вступление в силу 01.03.2028.

От монополии согласия к конкуренции оснований

2025: одно согласие, чтобы править всеми. 2026-2028: четыре равновеликих основания

Privacy Advocates

2025 Одно согласие, чтобы править всеми: универсальное и "безопасное" основание, которое легко взять и легко заменить.

2026-2028

Согласие

Исключение из правила

Ограниченный набор сценариев, повышенные требования к форме, оформлению и учету.

Договор

Средство, но не самоцель

Недопустимые условия, строгое потребительское регулирование, риск недействительности.

Законный интерес

Серая зона

Нет механизмов балансировки: нужна предварительная фильтрация обработок с дисбалансом интересов.

Обязанность

Публично-правовое основание

Отраслевые стандарты, госозера данных, предписания и запросы органов набирают вес.

Согласие как исключение из правила

Получение согласия предпочтительно в ограниченном наборе сценариев

Privacy Advocates

СЦЕНАРИИ, ГДЕ СОГЛАСИЕ УМЕСТНО

- включение ПД в общедоступные источники (ст.8 152-ФЗ)
- обработка специальных категорий ПД (ст.10 152-ФЗ)
- распространение ПД (ст.10.1 152-ФЗ)
- обработка биометрических ПД (ст.11 152-ФЗ)
- прямые маркетинговые и информационные контакты (ст.15 152-ФЗ)
- решения на основании автоматизированной обработки (ст.16 152-ФЗ)
- передача ПД работника (ст.88 ТК РФ)
- получение ПД работника не от него самого (ст.86 ТК РФ)

Антифрод-3 (проект от 30.09.2026): согласие и отзыв через ЕСИА, а требовать согласие, не предусмотренное законом или отраслевым актом, нельзя (ч.2.1 ст.18).

ВС РФ, 22.06.2026: встречное согласие на рекламу в обмен на скидку правомерно (дело Мэлон Фэшн Груп).

Открытый вопрос: согласие на обработку ПД не равно согласию на поручение обработки ПД (?)

Договор - средство, но не самоцель

Договорное основание под давлением потребительского регулирования

Privacy Advocates

НЕДОПУСТИМЫЕ УСЛОВИЯ ДОГОВОРА С СУБЪЕКТОМ ПД

- обработка ПД на основании договора, когда законом предусмотрено другое основание
- бездействие субъекта ПД как условие заключения договора
- обработка ПД, не требующихся для заключения и исполнения договора
- передача ПД неопределенному кругу лиц
- избыточный срок обработки ПД
- положения, ограничивающие права и свободы субъекта ПД
- обработка ПД несовершеннолетних в случаях, не предусмотренных законом

Антифрод-3: выделенные условия прямо запрещены новой редакцией п.5 ч.1 ст.6, а договор должен соответствовать отраслевому акту.

Потребительское регулирование: строгие правила заключения, исполнения, изменения и расторжения договоров с потребителями.

Риск недействительности: противоправность, мнимость, притворность, кабальность условий об обработке ПД.

Проблематика предмета: может ли обработка ПД быть самостоятельным предметом договора.

Туманный законный интерес: понять - значит упростить

Основание есть, механизма оценки и балансировки нет

Privacy Advocates

В российском праве нет механизмов оценки и балансировки законного интереса: результат оценки непредсказуем и неповторяем.

Законный интерес в серой зоне: ссылка на него не дает уверенности в законности, а явно незаконная обработка может им прикрываться.

Нужна предварительная отрицательная селекция обработок с дисбалансом интересов и дополнительные меры защиты субъектов.

Подтверждение неприменимости

п.7 ч.1 ст.6 152-ФЗ

три фильтра, которые обработка должна пройти, прежде чем опереться на законный интерес

Скачать

1 Допустимость *фильтр оснований*

- предусмотренное законом обязательное согласие на обработку ПД
- обработка ПД в случаях, прямо предусмотренных законом или договором

2 Правомочность *фильтр норм*

- отсутствие субъективных прав оператора или третьих лиц
- отсутствие норм права, определяющих общественный интерес

3 Пропорциональность *фильтр обработки*

- общедоступные источники ПД [ст.8 152-ФЗ]
- ПД недееспособных и несовершеннолетних [ст.9 152-ФЗ]
- специальные категории ПД [ст.10 152-ФЗ]
- ПД, разрешенные для распространения [ст.10.1 152-ФЗ]
- биометрия для установления личности [ст.11 152-ФЗ]
- трансграничная передача ПД [ст.12 152-ФЗ]
- маркетинг и агитация по каналам связи [ст.15 152-ФЗ]
- автоматизированное принятие решений [ст.16 152-ФЗ]
- ПД работников вне трудовых отношений [ст.86, 88 ТК РФ]
- изображение и частная жизнь [ст.152.1, 152.2 ГК РФ]
- ПД в составе охраняемой тайны [ст.9 149-ФЗ]

Отраслевые стандарты обработки ПД

Минимизация обработки через стандарты вместо согласий

Privacy Advocates

Милош Вагнер, 30.06.2025

"Строгие отраслевые стандарты должны определить перечень ПД и сроки их обработки, необходимые именно этому бизнесу именно в этой сфере отношений, что позволит исключить необходимость получения согласия человека на их обработку. Разрабатывать их будут профильные ведомства: здравоохранение, образование, финансы, ЖКХ и прочие - по согласованию с Роскомнадзором".

IV кв. 2026

План 2207-р, п.1

Ведомства определят объем ПД, необходимый бизнесу, и внесут предложения в Правительство.

22.07.2026

Проект Доктрины ИКТ

Сокращение оборота ПД за счет новых подходов к обработке и идентификации граждан.

19.08.2026

Инициатива

Ограничить хранение ПД пассажиров сервисами бронирования после передачи в госсистемы.

ВОЗМОЖНАЯ СТРУКТУРА ТИПОВОГО СТАНДАРТА

01

Процесс и параметры

цель, основание, категории субъектов, белый и черный списки ПД, источники, сроки, уничтожение, передача

02

Безопасность ПД

типовые перечни организационных, правовых и технических мер

03

Права субъектов

требования к порядку реализации прав субъектов ПД

Отраслевые акты вместо согласий

Антифрод-3 переносит идею отраслевых стандартов в ст.4 и ст.6 152-ФЗ

Privacy Advocates

Кто принимает: федеральные органы, отвечающие за политику и нормативное регулирование в своей сфере, обязаны (ч.2.1 ст.4), регионы, муниципальные органы и Банк России вправе (ч.2.2 ст.4).

Согласие
п.1 ч.1 ст.6

Договор
п.5 ч.1 ст.6

Законный интерес
п.7 ч.1 ст.6

ОТРАСЛЕВОЙ АКТ
для каждой цели задает

- состав ПД
- действия (операции)
- согласование с РКН до 60 дней (ч.3.1 ст.4)

Требовать нельзя, если согласие не предусмотрено законом или отраслевым актом (ч.2.1 ст.18); само согласие должно соответствовать акту.

Договор по акту: без условий, ограничивающих права субъекта, о случаях обработки ПД несовершеннолетних и о бездействии как условии заключения.

Законный интерес в рамке акта: состав ПД и действия для таких целей тоже определяет отраслевой акт.

Пояснительная записка: *сократить случаи избыточного сбора персональных данных на основании согласий на их обработку (в объеме, превышающем необходимый объем для осуществления хозяйственной деятельности соответствующих операторов).*

Дифференциация операторов ПД

Спецоператоры отложены, но не отменены

Privacy Advocates

Милош Вагнер, 24.09.2025

"Сейчас мы видим всего два препятствия для создания института спецоператоров: крупные компании, оказывающие услуги по защите персональной информации, завалены заказами на долгое время вперед, и им экономически нецелесообразно оказывать подобные услуги по более низкой стоимости сегменту МСБ. Социальная обязанность может быть навязана государством в какой-то момент времени. И, наверное, будет навязана. Но бизнес сам должен прийти к этому: каким бы крупным он ни был, утекают данные граждан его страны".

ПЛАН 2207-р, П.4

К III кварталу 2027 г. МВД, Минцифры, Минэкономразвития, ФСБ и РКН представят предложения о повышении ответственности и увеличении срока давности по нарушениям в области ПД.

КРИТЕРИИ СПЕЦОПЕРАТОРА ПО ИНИЦИАТИВЕ РКН (ОТ 100 ТЫС. ЗАПИСЕЙ)

- российское юридическое лицо
- не менее 5 штатных специалистов с высшим образованием в области ИБ
- финансовое обеспечение ответственности за утечку не менее 100 млн ₽
- базы данных только на территории РФ
- обработка с учетом требований по обеспечению ИБ

Защита ПД: ФСТЭК меняет поколение требований

Приказ № 117 уже действует, методдокумент задал каркас мер, приказ взамен № 21 пока проект

Privacy Advocates

11.04.2025 — подписан
Приказ № 117 взамен приказа № 17

01.03.2026 — в силе
Приказ № 117 вступил в силу

12.04.2026 — в силе
Методика ФСТЭК о составе мер

01.09.2026 — в силе
Приказ № 137, К(зи) с 01.03.2027

24.07.2026 — проект
Проект взамен приказа № 21

Приказ № 117: что уже действует

- область: любые ИС госорганов, учреждений и их подрядчиков; при ПД в ГИС - вместе с ПП-1119
- с 01.03.2027 К(зи) считает оператор раз в полгода с отчетом в ФСТЭК, У(зи) подрядчика - раз в два года
- уязвимости: критические - сутки, высокие - 7 дней; класс соотнесен с уровнем защищенности ПД

ПРОЕКТ ВЗАМЕН ПРИКАЗА № 21

- таблица мер по уровням исчезает: 21 мероприятие и 17 групп технических мер, состав оператор закрепляет в политике сам
- новые направления: ИИ, контейнеры, API, IoT, почта, веб, мобильные, DDoS, безопасная разработка, подрядчики, ГосСОПКА
- модель угроз - по решению оператора; срок 01.09.2026 не соблюден, состав мер пока задает приказ № 21

Оператору: новые системы - по новым требованиям, действующие - план перехода без аннулирования аттестатов; методика зрелости 07.08.2026 охватывает ИСПД; проект 24.08.2026 меняет блок ИИ.

От локализации к приземлению обработки ПД в РФ

Российское ПО, российские ЦОД, российские модели ИИ и российский контроль каналов

Privacy Advocates

01.09.2027

Иностранные облака и ПО

Минцифры предлагало запрет в ИСПД (кроме МСП, ИП и физлиц), но пока что законопроект публично не представлен.

265-ФЗ

Трансграничная передача

Конвенция 108 больше не гарантия адекватности; ориентир - перечень РКН (приказ № 253, с 30.10.2026: 88 государств, без Украины); РКН вправе запретить ТПД в любую страну.

43-ФЗ

Генетические данные

С 01.09.2026 передача за рубеж только для медпомощи, лекарств и международного сотрудничества, через Межведомственную комиссию либо в случаях п.4 Правил ПП-750 без нее.

243-ФЗ

Модели ИИ

Суверенные и национальные модели: российский разработчик и обработка данных в ЦОД на территории РФ; Правительство вправе делать их обязательными.

ФСТЭК · СОРМ

Защита и контроль каналов

Новое поколение требований ФСТЭК: приказ № 117 и проект взамен приказа № 21; приказ Минцифры № 1174 о СОРМ в технологических сетях включил паспорт, ИНН, реквизиты, IP, логины и геокоординаты.

Плюс 492-ФЗ: с 01.04.2026 органы ФСБ вправе получать по предписанию, без судебного решения, копии баз данных любых организаций. **Антифрод-3:** идентификация клиентов хостинга и заявление цели, требования к корпоративным VPN, виртуальные АТС только на российских IP.

Антифрод-2 принят, Антифрод-3 на подходе

Идентификация абонентов, детские сим-карты и новые составы КоАП

Privacy Advocates

15.04.2025

в силе

Антифрод-1 (41-ФЗ)

Ограничение массовых вызовов, маркировка звонков, самозапреты и первые антифрод-платформы.

26.06.2026

частично

Антифрод-2 (210-ФЗ)

До 20 карт на человека, компенсация похищенного, блокировка международных звонков, реестр IMEI, детские сим-карты; из пакета исключены Max, ИНН и согласия через ЕСИА.

07.07.2026

в силе

Санкции (199-ФЗ)

Ст.13.55 КоАП РФ - до 700 тыс. ₽ за неправильную авторизацию; ст.13.56 - до 2,8 млн ₽ за нарушения с рекомендательными технологиями.

01.03.2028

проект от 30.09.2026

Антифрод-3

Иностранным ресурсам - вход только по номеру, российским - четыре способа; 3 года хранения сведений о входах; согласия через ЕСИА; хостинг, VPN, смс без ПД адресата.

Детские сим-карты (проект правил, ред. 18.08.2026, на 30.09.2026 не принят): запрет смс-рассылок на детские сим-карты, включая коды регистрации и входа, кроме сообщений от ГИС; 55-ФЗ (с 05.09.2026) - поиск граждан через МВД без раскрытия ПД заявителю.

Календарь вступлений: что меняется до 2028 года

Ближайшие даты на октябрь 2026 года, сроки проектов условны

Privacy Advocates

ОКТЯБРЬ 2026 - МАРТ 2027

01.10.2026

Платформы

289-ФЗ: защита сведений и прозрачность автоматизации

30.10.2026

Перечень стран

приказ Роскомнадзора № 253: 88 стран вместо 89

01.01.2027

ЕБС

сегменты на векторах, конец переходной ПЭП

01.03.2027

ИИ и защита

243-ФЗ: суверенные модели, ФСТЭК № 137: К(зи)

01.03.2027

Связь и водители

210-ФЗ: информирующие вызовы, 200-ФЗ: медданные

СЕНТЯБРЬ 2027 - 2032

01.09.2027

Виды биометрии

истекает ПП № 408, виды для ЕБС определят заново

01.01.2028

Антифрод-2

последние этапы 210-ФЗ

01.03.2028

Антифрод-3

проект: вход по номеру, 3 года хранения сведений о входах

01.09.2032

Переход ИИ

конец перехода для систем на 01.03.2027

Авторизация пользователей: суть и статус изменений

ч.10 ст.8 149-ФЗ, санкции с 07.07.2026 и что меняет Антифрод-3

Privacy Advocates

Действующая норма

Владелец сайта, приложения или системы с российской аудиторией авторизует пользователей в РФ одним из четырех способов: абонентский номер, ЕСИА, ЕБС, иная система российского юрлица или гражданина РФ. Apple ID и Google Sign-In под запретом.

Границы требования

Критерий - местонахождение, а не гражданство; иностранные владельцы пока вне нормы; иностранная почта как логин - не нарушение; изъятий для внутренних и B2B-сервисов нет.

Ответственность

Ст.13.55 КоАП РФ (с 07.07.2026) - до 700 тыс. ₽ для юрлиц, отвечает владелец ресурса. С 01.09.2025 ст.13.29.2 - передача данных авторизации, до 200 тыс. ₽, ст.274.5 УК РФ - до 3 лет лишения свободы.

ПРАКТИКА

Литрес и VK Play убирают вход через Apple и Google ID, Ozon его отключил; открыты конфликт с п.4.8 правил App Store и судьба учетных записей.

АНТИФРОД-3, ПРОЕКТ ОТ 30.09.2026

Иностранным владельцам - только абонентский номер (ч.10.1-1), российским - четыре способа (ч.10.1); вернулось трехлетнее хранение сведений о регистрации и входах, а входы через ЕСИА хранит ЕСИА.

ЧТО ДЕЛАТЬ СЕЙЧАС

Сначала публичные ресурсы с видимой кнопкой иностранного входа, затем партнерские порталы и API, затем внутренние сервисы; коды входа генерировать и проверять на российской стороне.

Данные для государства: кто и что будет хранить

Цифровой оброк в Антифрод-3: журналы, адреса и идентификаторы

Privacy Advocates

КТО	ЧТО	КУДА И СКОЛЬКО	НОРМА
Владельцы сайтов, приложений и ИС	сведения о регистрации, авторизациях и прекращении регистрации	3 года, предоставление органам ОРД и безопасности; при входе через ЕСИА - в ЕСИА	**п.2 ч.10, ч.10.1-2 ст.8 149-ФЗ**
Операторы связи	сетевые адреса и порты при заключении договора через интернет	3 года у оператора связи	**пп.3 п.1 ст.64 закона о связи**
Юрлица и ИП с M2M и eSIM	номера, адреса абонента или установки, идентификаторы eSIM-оборудования	вносятся в ЕСИА, сведения по eSIM оператор проверяет до начала услуг	**п.1.1 ст.44 закона о связи**
Платформы с иностранными исполнителями	номера телефонов иностранных исполнителей	в ГИС по ст.44.2 закона о связи, сверку проводит РКН	**п.13 ст.13, ст.13.8 закона об иностранцах**
Хостинг-провайдеры	идентификация клиента и цель использования мощностей	проверка по реестру нарушителей до предоставления мощностей	**ч.5-5.4 ст.10.2-1 149-ФЗ**
ГИС Антифрод	сведения о причастных к нарушениям, включая данные для регистрации и входа	в порядке Правительства по согласованию с ФСБ	**ч.5 ст.1 41-ФЗ**

Для оператора ПД: необходимо документировать меры защиты и регламент предоставления органам ОРД и безопасности журналов/логов регистраций и авторизаций пользователей.

ИИ-регулирование 2026: что важно для обработки ПД

243-ФЗ, институции, стандарты и первая практика

Privacy Advocates

243-ФЗ от 26.07.2026, с 01.09.2026, часть норм с 01.03.2027

- впервые закреплены понятия ИИ, большой фундаментальной модели, набора данных, обучения и разработчика
- маркировка ИИ-контента добровольная
- использование объектов авторских прав для обучения выведено из состава нарушения только для суверенных и национальных моделей
- доступ разработчиков к наборам данных из ГИС не соотнесен с 152-ФЗ и режимом ИСПД - законность ПД в обучающих выборках открыта
- переход до 01.09.2032 для систем, действующих на 01.03.2027

Институции и стандарты: комиссия при Президенте по развитию технологий ИИ (Указ от 26.02.2026 № 116), подкомиссия Правительства, ГОСТ Р 72514-2026 "Оценка воздействия системы ИИ" на основе ISO/IEC 42005:2025.

На подходе: законопроект об ИИ в органах публичной власти (четыре уровня критичности, сертификация ФСТЭК и ФСБ, полигон Минцифры); законопроекты о дипфейках; предложение АБД о PETs без согласия для обучения ИИ.

Практика: 130-ФЗ запретил ИИ-образы и голоса в агитации; первая инстанция учла выгрузку тайны в нейросеть при увольнении (07.2026); использование ИИ не снижает гарантий для граждан (дело Дегустаторстрой).

Данные всегда переходят из слабых рук в сильные

Шесть трендов и их статус на осень 2026 года

Privacy Advocates

01

Ужесточение юридической ответственности за нарушения ПД

реализовано

02

Цифровой оброк для наполнения "госозера" данными

реализовано

03

Деприоритезация согласий как основания обработки ПД

проект Антифрод-3, Доктрина

04

Минимизация обработки ПД через отраслевые стандарты

проект Антифрод-3, 2207-р

05

Дифференциация операторов ПД по возможностям обработки

отложено

06

Переход от локализации 2.0 к приземлению обработки ПД в РФ

частично: 265-ФЗ, 243-ФЗ

Тенденция ближайших лет - концентрация обработки ПД в крупных структурах и перенос идентификации и согласий на государственную инфраструктуру (ЕСИА, ЕБС, ГИС Антифрод).

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
FIN-001	Чек-лист из основных контролей обработки и защиты ПД	Ресурсы и контакты
FIN-002	Дайджест значимых событий и инициатив в области ПД	Ресурсы и контакты

01.3

Антифрод-3

- Антифрод-3 в двух словах
- Авторизация: два режима и журналы входов
- Каналы и инфраструктура под контролем
- Антифрод-3 выходит за рамки борьбы с мошенниками: отдельный блок поправок в...

Антифрод-3 в двух словах

Третий пакет мер против правонарушений с использованием ИКТ: что в нем для ПД

Privacy Advocates

30.09.2026

проект опубликован для общественного обсуждения

01.03.2028

планируемое вступление в силу (ст.10 проекта)

9 законов

меняются одним пакетом, включая 152-ФЗ, 149-ФЗ и закон о связи

Проект и обсуждение regulation.gov.ru/projects/171465

ЧТО В ПАКЕТЕ ВАЖНО ДЛЯ ПД

152-ФЗ	согласие и отзыв через ЕСИА, сведения о согласиях в ЕСИА, жалобы через ЕПГУ, отраслевые акты о составе ПД, запрет требовать согласие сверх закона
149-ФЗ	для иностранных ресурсов вход только по номеру телефона, журналы входов 3 года, идентификация клиентов хостинга, требования к корпоративным VPN
О связи	смс без ПД адресата, идентификация абонентов через ЕСИА и ЕБС, сетевые адреса при онлайн-договоре 3 года, M2M и eSIM юрлиц в ЕСИА
41-ФЗ	ГИС "Антифрод" хранит сведения о причастных к нарушениям, включая данные для регистрации и входа

> **Мотив авторов:** после первого пакета доля ИКТ-преступлений снизилась в среднем на 12%, но схемы трансформируются и требуют новых мер (пояснительная записка).

Авторизация: два режима и журналы входов

Новая редакция ч.10-10.1-2 ст.8 149-ФЗ в проекте Антифрод-3

Privacy Advocates

РОССИЙСКИЕ ВЛАДЕЛЬЦЫ · Ч.10.1

любой из четырех способов

- Абонентский номер
- ЕСИА
- ЕБС
- Иная российская ИС

Нюанс: в ч.10.1 нет оговорки о пользователях в РФ, требование касается всех пользователей.

ИНОСТРАННЫЕ ВЛАДЕЛЬЦЫ · Ч.10.1-1

только абонентский номер

+7 для пользователей, находящихся в РФ; вход только через Apple ID или Google Sign-In больше не вариант

Сейчас иностранные владельцы вне ч.10 ст.8, по проекту изъятие для них исчезает.

ЖУРНАЛЫ ВХОДОВ · П.2 Ч.10 И Ч.10.1-2

Хранить 3 года

сведения о регистрации, авторизациях и прекращении регистрации пользователей

Предоставлять

органам ОРД и безопасности в составе и порядке, установленных Правительством

Вход через ЕСИА

сведения о таких авторизациях хранятся в ЕСИА, а не у владельца ресурса

Уже действует: ч.10 ст.8 в редакции 406-ФЗ и ст.13.55 КоАП РФ, до 700 тыс. ₽ для юрлиц с 07.07.2026.

Каналы и инфраструктура под контролем

Приземление в Антифрод-3: хостинг, VPN, телефония и рассылки

Privacy Advocates

Хостинг ст.10.2-1 149-ФЗ	Сервер в аренду дадут только после проверки личности клиента и цели аренды. VPN-сервисам, не подключенным к реестру запрещенных сайтов, откажут и на год внесут в черный список. При кибератаке сервер отключат по запросу силовиков.
Корпоративный VPN ч.18 ст.15.8 149-ФЗ	Сейчас VPN компании для своих сотрудников и рабочих задач выведен из-под требований к VPN-сервисам. Проект изъятие сохраняет, но Правительство с участием ФСБ установит к таким VPN требования и порядок уведомления РКН.
Виртуальные АТС ч.4.2 ст.10.2-1 149-ФЗ, п.12 ст.44 закона о связи	Облачные АТС, через которые бизнес звонит клиентам, будут размещать только на российских IP-адресах. Подключиться к такой АТС с зарубежного или не предназначенного для нее адреса не получится, оператор связи откажет в услуге.
СМС-рассылки ст.44.1 закона о связи	В смс нельзя будет упоминать имя и другие данные получателя и его родственников, если у отправителя нет права их использовать. Договор на рассылку заключит сама компания или мобильный оператор от ее имени, без агрегаторов.

Тренд приземления: контроль смещается с самих данных на каналы и инфраструктуру, через которые их обрабатывают, от сервера до смс.

КЛЮЧЕВЫЕ ВЫВОДЫ

- Антифрод-3 выходит за рамки борьбы с мошенниками: отдельный блок поправок в 152-ФЗ меняет сам институт согласия и основания обработки ПД.
- Согласие становится исключением: платформа на ЕСИА и ЕПГУ, типовые формы и запрет требовать согласие сверх закона и отраслевых актов.
- Минимизация через отраслевые акты переходит из планов в закон: состав ПД и действия для согласия, договора и законного интереса задаст ведомство по согласованию с РКН.
- Данные о пользователях уходят к государству: вход по номеру и ЕСИА, 3 года хранения сведений о входах, контроль хостинга, VPN и телефонии. Вступление в силу 01.03.2028, готовиться стоит уже сейчас.

КЛЮЧЕВЫЕ ВЫВОДЫ

- Ответственность и контроль стали жесткими и не всегда предсказуемыми: оборотные штрафы, ст.272.1 УК, риск-ориентированный надзор и дистанционный мониторинг, а с 2026 года - возврат дел в СОЮ и судебная линия "утечка не равна вине".
- Согласие теряет статус универсального основания: обособление формы, группа тяжести А, а Антифрод-3 добавляет платформу согласий на ЕСИА, отраслевые акты о составе ПД и запрет требовать согласие без обязанности.
- Приземление обработки идет по всем фронтам: перечень РКН для трансграничной передачи (265-ФЗ), генетические данные (43-ФЗ), суверенные модели ИИ (243-ФЗ), требования ФСТЭК уровня КИИ, СОРМ и право ФСБ на копии баз данных (492-ФЗ).
- Идентификация переходит к государству: авторизация по абонентскому номеру и ЕСИА, ЕБС, Антифрод-3 для иностранных ресурсов - концентрация обработки ПД в крупных и государственных структурах.

02

Этика и культура данных

Приватность, этика данных и культура работы с ними

02.1 Приватность и защита данных

02.2 Этика данных

02.3 Культура работы с данными

Раздел на сайте
privacy-advocates.ru/pd/eti

02.1

Приватность и защита данных

- Информационная приватность и защита данных пересекаются
- Приватность - это неприкосновенность частной и личной жизни
- ПД - любая информация, которую можно связать с человеком
- Частную жизнь охраняют запретом, а ПД - правилами оборота

Информационная приватность и защита данных пересекаются

Две рамки с общей зоной: что охраняет каждая и где они совпадают

Privacy Advocates

Информационная приватность

Личная сфера человека

ценности, важные человеку независимо от закона

- **уединение** - право побыть одному
- **близость** - круг, которому доверяют
- **тайна** - то, что не раскрывают
- **незаметность** - возможность не быть выделенным из толпы

и

Защита данных

Законный оборот данных

правила, по которым оператор отвечает перед субъектом и регулятором

- **подотчетность** - умение доказать соблюдение
- **законность** - основание и законная цель
- **добросовестность** - без обмана и сверх ожиданий
- **прозрачность** - понятное информирование

ОБЩАЯ ЗОНА ДВУХ РАМОК

минимизация | ограничение обработки | целостность | конфиденциальность

Вывод: защита данных задает правила законного оборота, а информационная приватность объясняет, зачем они нужны. Минимизация и безопасность работают на обе цели сразу

Приватность - это неприкосновенность частной и личной жизни

Калька с английского privacy: термин конца XIX века, ответ на развитие технологий и фотографии

Privacy Advocates

Желание уединиться и защитить личное пространство возникло как реакция на технологии, прежде всего на фотографию. Выделяют **четыре вида приватности**, и все они актуальны в цифровом мире

ст.22 Конституции

Телесная

неприкосновенность тела: осмотры, медицинские вмешательства, сбор биометрии

ст.25 Конституции

Пространственная

жилище, рабочее место и иное личное пространство, в том числе от наблюдения

ст.23 и 24 Конституции

Информационная

сбор, хранение, использование и распространение сведений о частной жизни без согласия не допускаются

ч.2 ст.23 Конституции

Коммуникационная

тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

Связь с ПД: режим оборота сведений о человеке, то есть информационной приватности, раскрывает 152-ФЗ, поэтому ПД - ее главный правовой инструмент

ПД - любая информация, которую можно связать с человеком

П.1 ст.3 152-ФЗ: информация о прямо или косвенно определенном или определяемом физическом лице

Privacy Advocates

П.1 СТ.3 152-ФЗ

Любая информация

относящаяся к прямо или косвенно определенному или определяемому физическому лицу

- **не только** сведения, которые точно идентифицируют конкретного человека, как паспорт или СНИЛС
- **а любые**, которые можно ассоциировать с человеком напрямую или через другие данные

ЧТО БЫВАЕТ ПД В ЗАВИСИМОСТИ ОТ КОНТЕКСТА

ФИО | дата рождения | возраст | серия и номер паспорта | ИНН | СНИЛС | адрес места жительства | номер телефона | e-mail | должность и место работы | фото- и видеоизображение | друзья и родственники | аккаунты соцсетей | логин учетной записи | IP-адрес | GA ID и IDFA | модель устройства | геолокация | ID в программе лояльности | количество баллов | история покупок | любимые товары | любимый магазин | рейтинг покупательских возможностей

Подробнее: отнесение сведений к ПД зависит от контекста и возможностей оператора, алгоритм и индекс атрибутивности разобраны в разделе 05 Определение ПД

Частную жизнь охраняют запретом, а ПД - правилами оборота

Два режима с разными подходом, методом, объектом, благом и способом защиты

Privacy Advocates

ПРИЗНАК	ЧАСТНАЯ ЖИЗНЬ	ПЕРСОНАЛЬНЫЕ ДАННЫЕ
Подход к регулированию	невмешательство и уважение	регулирование оборота
Метод регулирования	запрет	дозволение
Объект регулирования	особая сфера жизни	оборот данных
Защищаемое благо	нематериальное: достоинство	нематериальное: информация
Способ защиты	материальный: компенсация морального вреда	нематериальный: принципы обработки

ПАРАЛЛЕЛЬ

Две статьи - два предмета

Европейская модель разводит уважение к частной жизни (ст.7 Хартии ЕС об основных правах) и защиту ПД (ст.8 Хартии). По экспертному прочтению Россия следует тому же делению через ст.23 и 24 Конституции

Следствие: запрет защищает постфактум, через суд и компенсацию вреда, а дозволение задает заранее известные правила обработки, которые оператор обязан соблюдать и уметь доказать

Европейский стандарт защиты данных сложился в три поколения

От Конвенции о защите прав человека 1950 года до GDPR и Конвенции 108+, коротко

Privacy Advocates

1950

СОВЕТ ЕВРОПЫ

Конвенция о защите прав человека

ст.8 о частной жизни - ответ на злоупотребления тоталитарных режимов. До нее, в 1948 году, Всеобщая декларация прав человека ООН

1970-1973

ГЕССЕН, ШВЕЦИЯ

Первые законы о данных

эпоха мейнфреймов: данные обрабатываются свободно при основании, общих принципах и праве субъекта на доступ

1980-1981

ОЭСР, СОВЕТ ЕВРОПЫ

Первое поколение

Руководящие принципы ОЭСР и Конвенция № 108: понятия, принципы, права субъекта и свободная передача между странами

1995

ЕС

Второе поколение

Директива 95/46/EC: закрытый перечень оснований, согласие и независимый надзор на фоне интернета, прямого маркетинга и data mining

2016-2018

ЕС, СОВЕТ ЕВРОПЫ

Третье поколение

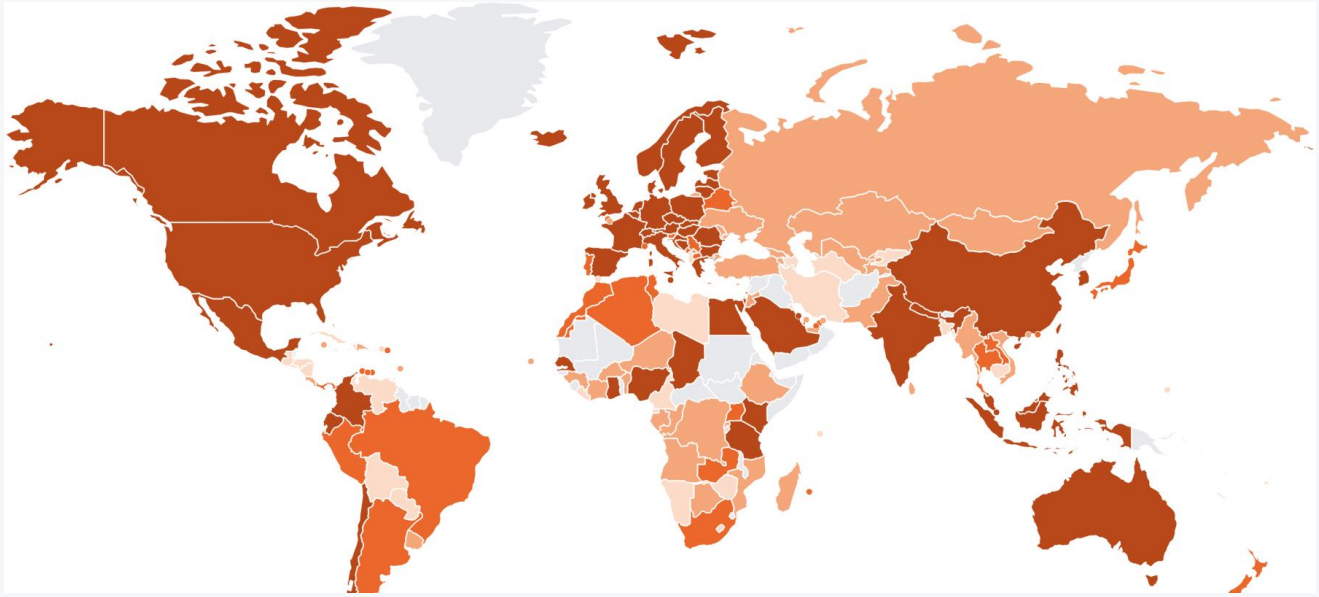
GDPR и Конвенция 108+: защита по оценке риска, уведомление об утечках, переносимость. Фон - соцсети, большие данные и разоблачения Сноудена

Для России: Россия ратифицировала Конвенцию № 108 (160-ФЗ от 19.12.2005, в силе для нее с 01.09.2013), а 152-ФЗ по содержанию относится ко второму поколению. Протокол 108+ на 13.10.2026 не вступил в силу: 34 ратификации из 38 нужных, подписание России приостановлено с 16.03.2022

Законы о ПД есть почти везде, но строгость разная

Карта DLA Piper 2026 года: 164 юрисдикции от ограниченного до жесткого регулирования

Privacy Advocates



От темного к светлому: жесткое (56), сильное (32), умеренное (43) и ограниченное (33) регулирование, серым - нет данных. Россия в группе умеренного

ТРИ МОДЕЛИ РЕГУЛИРОВАНИЯ

Европейская

единый закон для всех, независимый надзорный орган и приоритет прав человека

Американская

отраслевые федеральные законы и законы штатов, защита от вторжения в частную жизнь

Азиатская

близка к европейской, но приоритет у интересов государства, а не человека

Россия: российский закон европейский по происхождению, а по вектору развития ближе к азиатской модели: локализация баз и контроль трансграничной передачи

Конвенция № 108 остается основой российского закона

Конвенция Совета Европы 1981 года, Протокол № 223 (Конвенция 108+) и статус России на 2026 год

Privacy Advocates

28.01.1981

СТРАСБУРГ

Принята Конвенция № 108

первый международный договор о защите людей при обработке ПД

2005-2006

РОССИЯ

Ратификация и 152-ФЗ

Россия ратифицировала Конвенцию в 2005 году, а в 2006 году принят 152-ФЗ

01.09.2013

В СИЛЕ

Конвенция действует для России

и после исключения России из Совета Европы 16.03.2022

10.10.2018

КОНВЕНЦИЯ 108+

Протокол № 223

добавил согласие, уведомление об утечках, биометрию и генетику в чувствительные данные

2022-2026

СТАТУС

Протокол не вступил в силу

подпись России считается приостановленной с 16.03.2022

55

сторон Конвенции

46 государств Совета Европы и 9 государств вне его, в том числе Россия

34 из 38

ратификаций Протокола № 223

столько нужно, чтобы Конвенция 108+ вступила в силу

88

адекватных государств

после 265-ФЗ участие в Конвенции адекватности не дает, перечень задает приказ Роскомнадзора № 253 с 30.10.2026

Принципы обработки ПД можно объяснить человеческим языком

Десять человекочитаемых правил и нормы 152-ФЗ, которые за ними стоят

Privacy Advocates

1. **Прозрачность и подотчетность**
   скажите клиентам, что и зачем вы делаете с их данными. Без законной цели остальное неважно, ч.2 ст.5
2. **Ясность целей**
   говорите о целях понятным языком, без юридической чуши вроде "например, но не ограничиваясь", ч.2 ст.14
3. **Справедливость и законность**
   будьте конкретны: в цель "для улучшения пользовательского опыта" никто не поверит, ч.2 ст.5
4. **Ограничение обработки**
   доверие дано для конкретной цели, для новых целей его нужно заслужить или получить согласие, ч.2 ст.5
5. **Открытость передачи**
   сообщайте, когда делитесь данными с другими или получаете их не от самого клиента, ч.3 ст.18
6. **Минимизация**
   не откусывайте больше, чем можете или вам разрешено проглотить: ненужные данные не просите, ч.5 ст.5
7. **Конфиденциальность**
   берегите данные клиентов как свои, а их секреты - особенно надежно, ст.7, 10 и 11
8. **Качество и ограничение хранения**
   держите данные точными и актуальными, не становитесь складом или кладбищем данных, ч.6 и 7 ст.5
9. **Право знать и уйти**
   скажите клиенту, что о нем хранится, а если он уходит - отпустите и больше не беспокойте, ст.14 и 15
10. **Честность**
    если с данными что-то случилось, предупредите людей раньше, чем они столкнутся с проблемами. Закон требует уведомить Роскомнадзор (ч.3.1 ст.21), а людей - этика

Принципы 152-ФЗ повторяют европейские, но не все

Прозрачность и подотчетность в 152-ФЗ работают не как принципы, а через обязанности оператора

Privacy Advocates

ПРИНЦИП	КОНВЕНЦИЯ № 108	GDPR	152-ФЗ
Законность и справедливость	да	да	**ч.1 ст.5**
Прозрачность	да	да	**через обязанности**
Ограничение целями	да	да	**ч.2 ст.5**
Минимизация	адекватность и неизбыточность	минимизация данных	неизбыточность, ч.5 ст.5
Точность	точность и актуальность	точность и актуальность	точность, достаточность, актуальность, ч.6 ст.5
Ограничение хранения	да	да	**ч.7 ст.5**
Безопасность	отдельная статья	целостность и конфиденциальность	обязанности ст.7 и 19
Подотчетность	нет	да	**через обязанности**
Запрет объединять базы с несовместимыми целями	**нет**	**нет**	**ч.3 ст.5**

Права субъекта - это права людей, доверивших вам данные

Человекопонятные права и их опора в 152-ФЗ: что дает закон, а что остается этикой или GDPR

Privacy Advocates

ПРАВО	ПО-ЧЕЛОВЕЧЕСКИ	ОПОРА В 152-ФЗ
Гуманизм	это люди, такие же как вы, а не просто субъекты ПД: почаще ставьте себя на их место	этика
Справедливость	данные принадлежат людям, вам их дали подержать на время, и ваши права заканчиваются там, где начинаются их права	этика
Информирование	своевременно и доходчиво рассказывайте, что происходит с данными: неизвестность рождает недоверие и страх	ст.18, ч.2 ст.18.1
Доступ	доверяй, но проверяй: доступ к своим данным бесплатно, но без данных других людей	ч.2 ст.14, ч.1 ст.20
Исправление	Влад не хочет быть Вадимом: дайте исправить ошибки в данных	ч.1 ст.14, ч.2 ст.21
Удаление и блокирование	право на забвение, а на время переговоров хотя бы блокирование данных	ч.1 ст.14, ч.2 ст.9, ст.21
Возражение	против спама, особенно телефонного, и решения банковского "искусственного интеллекта" без человека	ст.15, ч.3 и 4 ст.16
Переносимость	не будьте тюрьмой для данных: дайте забрать копию и уйти в другой сервис	нет, это GDPR

02.2

Этика данных

- Этика данных надстраивается над юридическим минимумом
- Уважение к человеку за данными - первое начало этики
- Справедливость обработки проверяют постоянно
- Этическая подотчетность шире юридической

Этика данных надстраивается над юридическим минимумом

Этика данных - применение этических принципов при построении процессов обработки в организации

Privacy Advocates

КОДЕКС ЭТИКИ ДАННЫХ

Свой у каждой организации

Универсальных правил нет, поэтому организация пишет собственный кодекс. Он дополняет политики обработки и защиты данных и отражает ее культуру, ценности и цели

- дает единый ответ там, где ст.5 152-ФЗ оценочна
- заранее обозначает границу разумных ожиданий субъекта
- предъявляет эту границу вовне как обязательство

01

Уважение

к людям, которые стоят за данными

02

Справедливость

без предвзятости, дискриминации и изоляции

03

Подотчетность

открытая практика, механизмы управления и средства защиты

04

Прозрачность

обработка и решения объяснимы человеку

⚠ **Осторожно:** юридической силы кодекс не имеет, а расхождение практики с собственным кодексом работает против оператора. Принимают только те начала, которые готовы соблюдать и контролировать

Уважение к человеку за данными - первое начало этики

Организация отвечает за общепризнанные права человека, а не только за соблюдение 152-ФЗ

Privacy Advocates

ПРАВА, ЗА КОТОРЫЕ ОТВЕЧАЕТ ОРГАНИЗАЦИЯ

- неприкосновенность частной жизни
- достоинство
- разнообразие
- справедливость
- равенство
- автономия
- свобода от принуждения
- свобода от слежки
- свобода от обмана и манипуляций

К ЧЕМУ СТРЕМИТЬСЯ

- понимать и уважать интересы всех сторон
- использовать данные так, чтобы выгоду получали и сами люди
- понимать воздействие на людей и снижать риск вреда
- уважать автономию: реальный выбор и контроль, а не их имитация

Убеждение: выбор за человеком

- отказаться так же легко, как согласиться
- необязательная обработка заранее не включена

vs

Манипулирование: выбор смещен интерфейсом

- отказ спрятан глубже, чем согласие
- отметка в пользу необязательной обработки стоит по умолчанию

Спорно: общего теста для разграничения нет ни в законе, ни в практике. Прямо закреплено, что молчание не согласие на распространение (ч.8 ст.10.1), и запрещены заранее проставленные отметки о допуслугах в потребкредите (ч.2 ст.7 353-ФЗ)

Справедливость обработки проверяют постоянно

Данные способны и включать, и изолировать: адресная реклама дискриминирует и позитивно, и негативно

Privacy Advocates

ЧЕТЫРЕ ЭЛЕМЕНТА СПРАВЕДЛИВОСТИ

Наборы данных

без предвзятости, неточности и неактуальности выборки

Образ мышления

без дискриминации и изоляции людей, особенно уязвимых групп

Управление

разнообразие взглядов и опыта в командах, которые решают об обработке

Доступ и возможности

инклюзивность результата для тех, кого он затрагивает

ЮРИДИЧЕСКИЙ ВЫХОД

Ч.1 и ч.6 ст.5 152-ФЗ

Предвзятый или устаревший набор нарушает требование точности, достаточности и актуальности данных и оценивается через справедливость обработки

- проверяйте наборы для значимых решений периодически: смещение копится незаметно
- фиксируйте дату и результат проверки - это доказательство добросовестности
- привязывайте периодичность к темпу обновления данных и весу решений

Этическая подотчетность шире юридической

Давление на бизнес растет со стороны все более широкого круга заинтересованных сторон

Privacy Advocates

Черты этичной работы

Что должно быть в организации

- открытая и прозрачная практика работы с данными
- надежные глобальные и локальные механизмы управления
- действенные средства защиты и возмещения при нарушении этических принципов, а не только закона
- обратная связь: люди могут спросить и возразить по этическим и юридическим основаниям

vs

Канал этического возражения

Спор внутри, а не у регулятора

- закон дает оспорить правомерную обработку только по установленным поводам, кодекс - и формально законную, но несправедливую
- такое возражение доходит до оператора раньше жалобы в Роскомнадзор или публичного скандала
- нужно определить, кто рассматривает возражение, в какой срок и вправе ли он прекратить законную обработку

Совет: статистика этических возражений - ранний индикатор расхождения практики с ожиданиями аудитории, он срабатывает раньше жалоб и претензий

Решения на данных должны быть объяснимы человеку

Цели, выгоды и риски обработки понятны людям, а обоснованность решения можно проверить

Privacy Advocates

Прозрачность значит, что обработка и автоматизированные решения **имеют смысл для людей**: человек понимает цели и выгоды обработки, свои риски, социальные и этические последствия

ГДЕ СТАВКИ ОСОБЕННО ВЫСОКИ

Диагноз

медицинская диагностика

Кредит

решение о выдаче кредита

Работа

возможность трудоустройства

В 152-ФЗ

Ст.16: решения без человека

Решение с юридическими последствиями, основанное исключительно на автоматизированной обработке, допустимо только с письменного согласия субъекта или в случаях, предусмотренных законом

- оператор разъясняет порядок и последствия решения и дает возможность возразить, ч.3
- возражение рассматривают в течение 30 дней, ч.4

Важно: в ИИ и машинном обучении решение не всегда легко объяснить, поэтому его обоснованность должна поддаваться независимой и беспрепятственной проверке

Этика ИИ прошла путь от руководства ЕС 2019 года к законам

Ethics Guidelines for Trustworthy AI: необязательная рамка, которая сформировала регулирование ИИ

Privacy Advocates

06.2018

ЕВРОКОМИССИЯ

Группа AI HLEG

независимая группа экспертов высокого уровня по ИИ создана в рамках стратегии ИИ ЕС

04.2019

AI HLEG

Руководство по этике

не три закона робототехники Азимова, а анализ этических аспектов ИИ в здравоохранении, образовании и потреблении

01.08.2024

ЕС

Регламент об ИИ

Регламент 2024/1689 вводится поэтапно до августа 2028 года и применяется параллельно с GDPR

09.07.2025

БАНК РОССИИ

Кодекс этики ИИ

информационное письмо ИН-016-13/91 о кодексе этики в сфере ИИ на финансовом рынке

01.09.2026

РОССИЯ

Закон 243-ФЗ

о поддержке развития технологий ИИ в силе, часть норм, включая предупреждение об ИИ-материале, с 01.03.2027

Вывод: руководство не имело обязательной силы, но задало рамку, на которую опирается регулирование. Рамочный закон об ИИ 243-ФЗ действует с 01.09.2026, но в проектах с моделями основная нагрузка по-прежнему лежит на нормах о ПД

02.3

Культура работы с данными

- Культура данных ставит данные выше мнения начальника
- Культура данных начинается с договоренности внутри компании
- Работу с данными ведут четыре группы с разными интересами

Культура данных ставит данные выше мнения начальника

Модель HiPPO против Data-Driven culture: что на самом деле решает в компании

Privacy Advocates

Культура работы с данными - принцип, при котором все сотрудники, особенно лица, принимающие решения, при изменениях и решениях **в первую очередь ориентируются на данные** и результаты их анализа

HiPPO

Мнение самого высокооплачиваемого

Highest Paid Person's Opinion

- решают интуиция и опыт руководителя
- статистику учитывают, но последнее слово за мнением
- модель остается популярной и в XXI веке

vs

Data-Driven

Культура работы с данными

Data-Driven culture

- оперативные и стратегические решения опираются на данные и результаты их анализа
- в основе - объективность и значимость собранных данных
- подход не революционный: доходы и расходы считали и раньше, меняется вес данных в решении

Связь с приватностью: этические начала остаются декларацией, если в организации нет культуры работы с данными: она и есть среда соблюдения требований приватности

Культура данных начинается с договоренности внутри компании

Пререквизит: мы договорились, что данные могут дать хороший ответ или совет в дилемме

Privacy Advocates

Из такой договоренности следуют **четыре готовности** - без них дашборды и отчеты остаются картинками

1

Инвестировать

деньги и время в извлечение, хранение, анализ, интерпретацию и визуализацию данных

2

Слушать

перед решением остановиться и сказать себе: давайте посмотрим на числа

3

Понимать

неверный вывод из верных цифр сделать ужасающе просто, нужен минимум аналитического мышления у тех, кто решает

4

Доверять

руководствоваться данными при решениях, но помнить, что аналитики могли не учесть сезонность, выборы или иное

Важно: менеджер, который поступает по опыту вопреки отчету, не обязательно неправ: решает диалог и взаимное доверие менеджеров и аналитиков

Работу с данными ведут четыре группы с разными интересами

Каждая группа считает главной свою часть работы, и все они - элементы Data-Driven культуры

Privacy Advocates

Аналитики

Ищут ответы

финансисты, экономисты, маркетологи: исследуют, выявляют причины и влияние факторов, например на рост себестоимости

Технари

Строят алгоритмы

разработчики баз данных, математики, Data Science: хранилища, алгоритмы и автоматизация отчетов без сбоев

Визуалы

Делают понятным

превращают таблицы в диаграммы, слайды и дашборды, ставят задачи дизайнеру и разработчику

Заказчики

Ждут выводов

руководителям нужны не графики, а варианты решений и прогнозы простым языком, например какие цены дадут максимум продаж

Для приватности: требования к обработке исполняет каждая группа, а адресуют их обычно только заказчику. Доводите их до всех напрямую (п.6 ч.1 ст.18.1 152-ФЗ): о лишнем атрибуте, сроке жизни выгрузки и получателях решают там, где обрабатывают данные

Приватность и культура данных сходятся в Privacy by Design

Выводы раздела: лучший способ снизить риски приватности - не создавать их

Privacy Advocates

По философии Privacy by Design чем меньше данных оператор собирает и обрабатывает, тем **меньше риск нарушить права субъектов** и причинить ущерб самому оператору. Стратегии проектируемой приватности делятся на две группы

ОРИЕНТИРОВАННЫЕ НА ПРОЦЕССЫ

Организационные стратегии

определяют процессы, которые обеспечивают ответственное управление ПД: кто и в каком порядке отвечает за данные

СТРАТЕГИЯ НА ДАННЫЕ	ЧТО ДЕЛАЕТ С НАБОРОМ ПД
Минимизация, minimise	ограничивает сбор, исключает избыточные ПД из наборов и удаляет или уничтожает их
Сокрытие, hide	смешивает, запутывает, маскирует или ограничивает доступ, чтобы ПД не раскрыли неправомерно
Отделение, separate	хранит наборы обособленно, чтобы затруднить их сопоставление и объединение
Объединение, aggregate	агрегирует и группирует ПД, снижая детализацию до уровня, который еще дает пользу

Итог раздела: культура данных без приватности дает эффективность ценой доверия, а приватность без культуры дает комплаенс, которого никто не исполняет

ЧАСТЬ

II

Фундамент комплаенса ПД

Что считается ПД и когда их обработка допустима

03 Обзор комплаенса ПД
04 Осведомленность персонала
05 Определение ПД
06 Допустимость обработки ПД

03

Обзор комплаенса ПД

Жизненный цикл обработки ПД за один проход: от определений до ответственности

03.1 Что и кем регулируется

03.2 Основания и согласие

03.3 Движение данных

03.4 Хранение и уничтожение

03.5 Система комплаенса

03.6 Инциденты и ответственность

Раздел на сайте
privacy-advocates.ru/pd/baz

03.1

Что и кем регулируется

- Обзор идет по пути ПД: от сбора до ответственности
- Что такое обработка ПД?
- Автоматизированная и неавтоматизированная обработка
- Основные действующие лица

Обзор идет по пути ПД: от сбора до ответственности

Шесть шагов жизненного цикла: номер открывает подраздел, плашка ведет в профильный раздел

Privacy Advocates

ШАГ	ЧТО РАЗБИРАЕМ	ГЛУБЖЕ В РАЗДЕЛАХ
03.1	**Что и кем регулируется** обработка, роли участников, регулирование и надзор	05 Определение ПД · 17 Права субъектов · 29 РКН и органы
03.2	**Основания и согласие** письменная форма, спецкатегории, биометрия, ПД детей	06 Допустимость · 10 Основания · 12 ПД потребителей · 15 Биометрия
03.3	**Движение данных** поручение, распространение, ТПД и локализация	14 Распространение · 19 Локализация · 20 ТПД · 21 Поручение и DTA
03.4	**Хранение и уничтожение** процессы, сроки хранения, уничтожение	18 Уничтожение ПД
03.5	**Система комплаенса** гэп-анализ, ответственный, риски, уведомление РКН	07 Организация · 22 Сайт · 26 Прайваси-риски · 29 РКН и органы
03.6	**Инциденты и ответственность** инцидент, оценка вреда, штрафы и ст.272.1 УК	28 Инциденты · 30 Ответственность

Что такое обработка ПД?

Любое действие с ПД с использованием средств автоматизации или без них (п.3 ст.3 152-ФЗ)

Privacy Advocates



1. **Сбор, запись**
2. **Систематизация, накопление, хранение**
3. **Уточнение, извлечение, использование**
4. **Передача: распространение, предоставление, доступ**
5. **Обезличивание, блокирование**
6. **Удаление, уничтожение**

Ресурсы, где хранятся ПД

Информационные системы

- Базы данных
- Серверы
- Рабочие станции
- Сетевая инфраструктура

Бумажные носители

- Журналы
- Анкеты
- Визитные карточки
- Договоры

Электронные носители

- Магнитные ленты
- Флеш-носители
- Оптические диски

Автоматизированная и неавтоматизированная обработка

ч.1 ст.1 и п.4 ст.3 152-ФЗ, ПП-687: граница и последствия

	С использованием средств автоматизации	Без использования средств автоматизации
Алгоритм	задан	задан
Операции	любые, участие человека не обязательно для каждой операции	использование, уточнение, распространение и уничтожение по каждому субъекту - при участии человека (п.1 ПП-687)
Средства	ИС, сети, АРМ, машинные носители	бумажные носители и систематизированные картотеки, в том числе квазиавтоматизированные

Бумажный контур по ПП-687

- ПД обособляются от иной информации, на одном носителе нет данных с несовместимыми целями
- носители по разным целям хранятся раздельно, места хранения и допущенные лица определены
- типовые формы документов и журналы пропуска ведутся по пп.7-8 ПП-687
- вне ст.1 лишь устное сообщение и несистематизированная бумага, граница спорна

ЛОВУШКИ И СПОРНАЯ ГРАНИЦА

- **РКН 01.07.2026:** ПК, 1С, документы по почте - уже автоматизация, изъятие п.8 ч.2 ст.22 не работает
- **9 ААС, А40-12676/2024:** сбор через форму на сайте сам по себе не автоматизация, если данные обрабатывает человек
- **АС МО 27.03.2025:** вывод назван верным, но акт апелляции отменен

Широкое прочтение РКН не бесспорно, но опора на это дело рискованна

Основные действующие лица

Четыре роли в обработке ПД и их правовой статус

Privacy Advocates

ЦЕНТРАЛЬНАЯ РОЛЬ

Оператор ПД

Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПД, а также определяющие цели обработки, состав ПД и действия (операции), совершаемые с ПД

Цели **Состав ПД** **Действия**

п.2 ст.3 152-ФЗ

Субъект ПД

п.1 ст.3 152-ФЗ

Физическое лицо, к которому относятся соответствующие ПД

Обработчик ПД

нет в 152-ФЗ как статуса

Оператор, действующий в интересах и по поручению другого оператора на основании договора о поручении обработки (ч.3 ст.6 152-ФЗ)

Получатель ПД

нет в 152-ФЗ как роли

Лицо или орган, которому передаются ПД. Получив ПД не от субъекта, уведомляет его до начала обработки (ч.3, 4 ст.18 152-ФЗ)

Кто может быть субъектом ПД?

47 категорий субъектов в 5 группах: основа перечня для большинства организаций

Privacy Advocates



Соискатели и связанные лица
5 категорий

- Соискатели на вакансии
- Рекомендатели
- Члены семьи соискателей
- Кадровый резерв

Персонал, владельцы и связанные лица
16 категорий

- Работники
- Бывшие работники
- Стажеры
- Владельцы
- Курьеры и ГПХ-подрядчики
- Родственники работников

Контрагенты и связанные лица
9 категорий

- Клиенты и потенциальные клиенты
- ИП и самозанятые
- Представители контрагентов
- Застрахованные лица

Взаимодействующие лица
9 категорий

- Пользователи сайтов и приложений
- Получатели рассылок
- Участники мероприятий и акций
- Посетители офисов

Иные категории
8 категорий

- Потребители
- Пациенты
- Специалисты здравоохранения
- Госслужащие
- Пользователи продукции

Каталог категорий субъектов ПД

privacy-advocates.ru/pd/katalog_subektov

Актуальность: 15.11.2025

Перечень не исчерпывающий и требует адаптации под деятельность оператора

ДВОЙНОЙ СТАТУС ИП

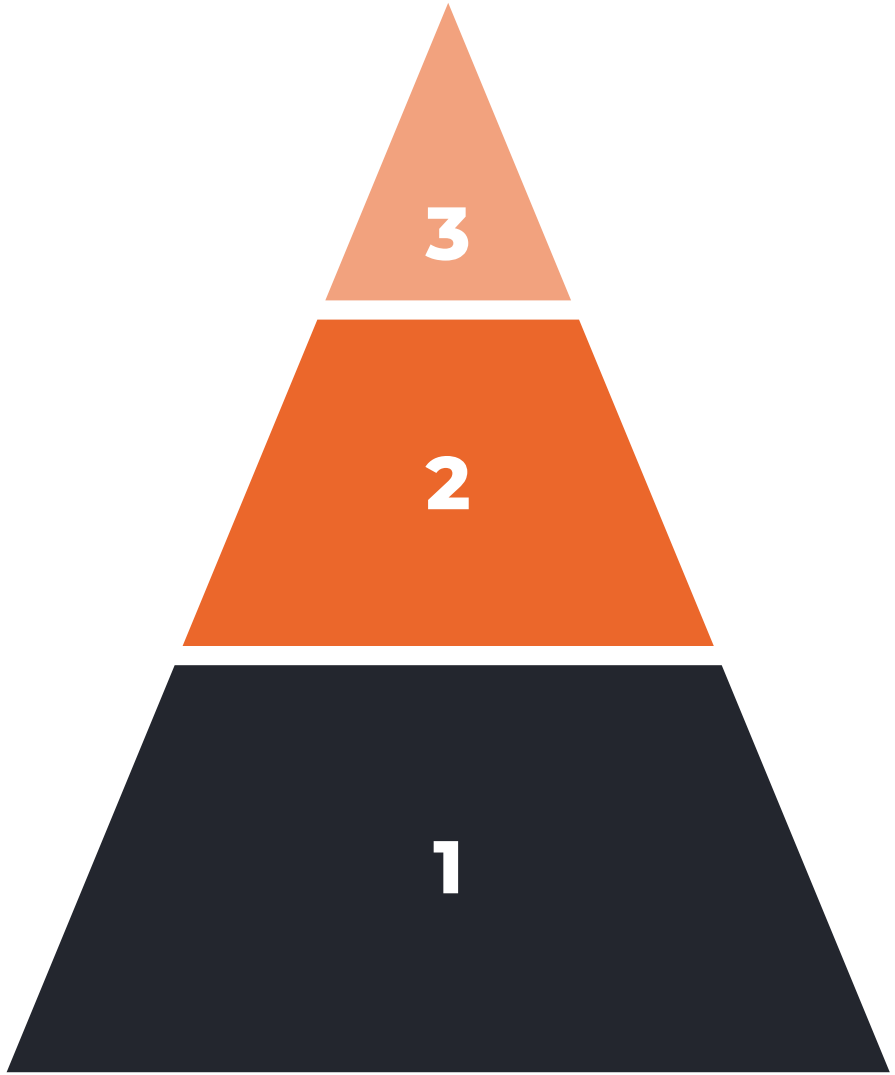
ИП одновременно субъект ПД и оператор ПД как субъект экономической деятельности

Чем в действительности регулируется обработка ПД

Нормы, практика и позиции регулятора

Материалы РКН
скачать

Privacy Advocates



Слово регулятора

устные позиции на днях открытых дверей и встречах, предостережения и предписания

Практика

письменные разъяснения РКН и Минцифры, проверочные листы, судебная практика

Нормы

152-ФЗ, 149-ФЗ, ТК, ГК, ПП-1119, ПП-687, ПП-1046, приказы РКН № 18, 140, 178, 179, 180, 187, ФСТЭК № 21 и 117, ФСБ № 378 и 77

ПЛАСТЫ РЕГУЛИРОВАНИЯ

Конституционный
ст.23-24: частная жизнь, личная и семейная тайна

Информационный
149-ФЗ: ограничение доступа и конфиденциальность

Специальный
152-ФЗ: режим ПД, права субъектов, обязанности оператора

Гражданско-правовой
гл.8 ГК: частная жизнь, изображение (ст.152.1)

Отраслевой
банковская и врачебная тайна, тайна связи, гл.14 ТК

Подзаконные акты обязательны в пределах закона. Разъяснения и устные позиции суд не связывают, но показывают, как поведет себя надзор.

Кто контролирует оператора ПД

Разные органы, разный предмет и разные рычаги воздействия

Privacy Advocates

Роскомнадзор
защита прав субъектов: проверки, профвизиты, дистанционный контроль, дела по ст.13.11 КоАП

ФСТЭК России
техзащита: приказы № 21 и 117, сертификация СЗИ, контроль мер ст.19 в госсистемах (ч.8 ст.19)

ФСБ России
криптозащита (приказ № 378), ГосСОПКА, предписания о доступе к ИС и копиях баз

Прокуратура
общий надзор вне ограничений 248-ФЗ, возбуждает дела по ст.13.11 КоАП

Оператор ПД

ПЯТЬ ФОРМ ВЗАИМОДЕЙСТВИЯ

1. проверки по 248-ФЗ
2. мероприятия без взаимодействия
3. профилактический визит
4. обращения граждан и запрос по ч.4 ст.20
5. прокурорский запрос (ст.17.7 КоАП)

Минцифры России
регулирование: биометрия и ЕБС, обезличивание и НСУД, законопроекты

Банк России
финрынок: инциденты через ФинЦЕРТ, стандарты ИБ, биометрия финрынка

ФАС России
реклама: рассылки и звонки без согласия по ст.18 закона о рекламе

Роспотребнадзор и Роструд
навязанное согласие в договоре с потребителем, кадровые ПД по гл.14 ТК

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OPR-001	Что есть ПД: пять стадий принятия неизбежного	05 Определение ПД
OPR-002	Дефиниция ПД и идентификатора	05 Определение ПД
OPR-010	Правоприменительная практика по определению ПД	05 Определение ПД
OPR-011	Мерцающие ПД	05 Определение ПД
OPR-018	Алгоритм определения ПД: принципы	05 Определение ПД
OPR-019	Алгоритм определения ПД: механика	05 Определение ПД
OPR-020	Индекс атрибутивности данных: описание и параметры	05 Определение ПД
OPR-021	Индекс атрибутивности данных: основные преимущества	05 Определение ПД
OPR-022	Индекс атрибутивности данных	05 Определение ПД
OPR-013	Каталог групп персональных данных	05 Определение ПД
OPR-014	Виды ПД по способам их получения	05 Определение ПД
SUB-003	Из семи сроков исполнения требований продлевают только десятидневный	17 Права субъектов

03.2

Основания и согласие

- Когда нужна письменная форма согласия
- Специальные категории ПД: закрытый перечень
- Биометрия после 572-ФЗ: два контура
- ПД несовершеннолетних: возраст решает форму

Когда нужна письменная форма согласия

Закрытый перечень случаев, шесть критериев и обособление с 01.09.2025

Схема свойств согласия
скачать

Privacy Advocates

Шесть критериев
свободно и в своем интересе плюс пять признаков ч.1 ст.9

- конкретность
- предметность
- информированность
- сознательность
- однозначность
- добровольность

ОБЫЧНАЯ ФОРМА

Любой подтверждаемый способ

- активная отметка в веб-форме, устно с записью, конклюдентно
- доказывание лежит на операторе: журнал событий с датой, временем, текстом и идентификатором
- скриншотов с пояснениями оператора для суда мало
- отметка в интерфейсе не является электронной подписью

ПИСЬМЕННАЯ ФОРМА, ч.4 ст.9

Только там, где ее прямо требует закон

Специальные категории
ст.10 152-ФЗ

Биометрия
ст.11 152-ФЗ

Общедоступные источники
ст.8 152-ФЗ

Автоматизированные решения
ст.16 152-ФЗ

ПД работника у третьих лиц
п.3 ст.86 ТК

Передача ПД работника
ст.88 ТК

Реквизиты по ч.4 ст.9, в электронной форме - с электронной подписью

Специальные категории ПД: закрытый перечень

Шесть типов сведений ч.1 ст.10 152-ФЗ и судимость с собственным режимом

Каталог ПД на сайте

Privacy Advocates



Судимость - отдельный режим ч.3 ст.10

Перечень закрыт

Имущественное положение и кредитная история остаются обычными ПД, генетика и биометрия живут по своим режимам. Расширить перечень толкованием нельзя, как и занизить режим.

Вывод тоже спецкатегория

Если из покупок, геолокации или поискового профиля выводится здоровье или убеждения, производные сведения обрабатываются по правилам ст.10.

Фото решает цель

Изображение лица становится спецкатегорией, когда обрабатывается специально для определения расы, национальности или убеждений.

Основание - письменное согласие (ч.4 ст.9) либо случаи ч.2 ст.10. С 30.05.2025 утечка спецкатегорий наказывается по ч.16 ст.13.11 КоАП: **10-15 млн ₽** независимо от объема, повторно по ч.18 - 1-3% выручки.

Биометрия после 572-ФЗ: два контура

Единая биометрическая система или собственная обработка по ст.11 152-ФЗ

Privacy Advocates

КОНТУР ЕБС

572-ФЗ: изображение лица и голос

- **Идентификация** (1 к N, кто это?) только через ЕБС: собственная биометрическая идентификация в системах организаций запрещена (ст.15)
- **Аутентификация** (1 к 1, ты ли это?) по векторам ЕБС через аккредитованную организацию, офису собственная аккредитация не нужна
- Первичный сбор только уполномоченные организации (МФЦ, банки) и приложение Госуслуги Биометрия, свой терминал регистрации недопустим
- ПП-1912 (с 01.03.2026) сохранило заселение через ЕБС, с 01.04.2026 и по документу из Госуслуг. С 01.01.2027 региональные сегменты только с векторами

VS

КОНТУР СТ.11 152-ФЗ

Все, что вне 572-ФЗ

- Отпечатки, рисунок вен, радужка (вне перечня ПП-408) и сверка с участием должностного лица
- Письменное согласие отдельным документом, конкретному оператору, обработчики поименно
- Отпечатки ради пропуска работодатель снимать не вправе (Роструд), после увольнения биометрия уничтожается
- Не биометрия: подсчет посетителей, контроль СИЗ, транскрибация встреч без установления личности
- Утечка биометрии - ч.17 ст.13.11 КоАП: 15-20 млн ₽ независимо от объема

Запрет понуждения

нормы и санкции

ч.3 ст.11 152-ФЗ

нельзя отказать в обслуживании из-за отказа дать биометрию

чч.11-13 ст.3 572-ФЗ

нельзя обусловливать услуги и продажу товаров биометрией

ч.2.1 ст.5.63, ч.8 ст.14.8 КоАП

за отказ в госуслуге чиновнику до 25 тыс. ₽, за отказ потребителю юрлицу 200-500 тыс. ₽

ПД несовершеннолетних: возраст решает форму

Кто дает согласие и где в 2026 году выросли риски

Комментарий к 266-ФЗ
скачать

Privacy Advocates

до 14 лет

Согласие дает законный представитель, он же реализует права субъекта. Общий кадр с публичного мероприятия - без согласия в рамках изъятий ст.152.1 ГК (РКН, 01.03.2023).

14-18 лет

Сам - только в случаях ст.26 ГК (РКН, 14.08.2026), прежние устные позиции расходились. Счет 14-летнему без согласия отца: банку штраф 150 тыс. ₽ (дело 12-2573/2026).

18 лет и старше

Выросший субъект вправе отозвать согласие и требовать удаления данных, собранных в детстве, через общие механизмы ст.14 и 21 152-ФЗ.

УГОЛОВНЫЙ ТРЕК

ч.2 ст.272.1

Незаконный оборот данных детей - квалифицированный состав наравне со спецкатегориями и биометрией: до 5 лет лишения свободы.

Детские сим-карты

С 01.03.2027 абонент вправе сообщить оператору связи, что номером пользуется ребенок (210-ФЗ от 26.06.2026). Проект правил запрещает слать на него коды входа и иные SMS.

Маркетинг и профилирование

Прямой маркетинг ребенку только с предварительного согласия (ч.1 ст.15), профилирование детей - зона повышенного риска.

Оценка вреда

Обработка ПД несовершеннолетних по договору с ними вне случаев закона дает высокую степень вреда (приказ РКН № 178).

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
KAD-004	Риск по согласию зависит от способа, формы и фиксации	11 ПД работников
BIO-030	Режим задают установление личности и биораспознавание	15 Биометрия

03.3

Движение данных

- Взаимодействие между основными лицами
- Поручение или передача: что фиксирует соглашение
- Распространение ПД: тест двух звеньев
- Трансграничная передача ПД: что это и куда

Взаимодействие между основными лицами

Кому оператор поручает обработку, а кому передает ПД

Privacy Advocates

Субъект предоставляет ПД оператору

Оператор ПД

Поручение обработки

Определяет обработчика ПД, гарантирующего принятие технических и организационных мер безопасности при обработке ПД

Оператор и обработчик должны заключить договор о поручении обработки ПД

Ответственность перед субъектом за действия обработчика несет оператор (ч.5 ст.6 152-ФЗ)

Передача ПД

Определяет получателя ПД (в т.ч. другого оператора) для передачи ему ПД

Оператор и получатель могут заключить договор о передаче ПД без поручения обработки

Для передачи нужно самостоятельное правовое основание обработки

Поручение или передача: что фиксирует соглашение

Тест собственной цели, обязательные условия и распределение ответственности

Сравнение соглашений о ПД
скачать

Privacy Advocates

ПОРУЧЕНИЕ ОБРАБОТКИ (ч.3 ст.6)

Обработчик действует в чужих целях

- перечень действий и цели обработки
- конфиденциальность и меры защиты по ст.19, уровень защищенности
- локализация по ч.5 ст.18 в редакции с 01.07.2025
- сообщение об инциденте заметно раньше 24 часов оператора
- подтверждение уничтожения, право на аудит, условия субобработки

Перед субъектом за обработчика отвечает оператор (ч.5 ст.6), за иностранного обработчика - оба (ч.6 ст.6). Аутсорсинг: кадры, бухгалтерия, хостинг.

?

есть ли у получателя своя цель

ПЕРЕДАЧА ПД (без поручения)

Получатель - самостоятельный оператор

- рамочное межоператорское соглашение, взаимное и равноправное
- правомерность передачи: согласие или иное основание ч.1 ст.6
- конфиденциальность (ст.7) и безопасность (ч.1 ст.19) у каждой стороны
- информирование субъектов и порядок реагирования на их запросы

Краткосрочный аутсорсинг с контролем результата: зарплатный проект, страхование, связь, медосмотры.

Хостинг и техподдержка сайта

регулятор квалифицирует как поручение (дело А49-14214/2022)

Мощности без доступа к данным

РКН устно относит к поручению (14.08.2026), экспертно - четыре признака обработчика, включая доступ

Обязанность по закону у каждого

поручения нет, каждый обрабатывает в силу своей обязанности (пример - клиринг)

Распространение ПД: тест двух звеньев

Где кончается предоставление определенному кругу и начинается раскрытие неопределенному

Privacy Advocates

Раскрытие ПД (п.5 и п.6 ст.3 152-ФЗ)

1 Установлен ли допуск?

Можно достоверно определить перечень лиц, имевших право доступа в конкретный момент или период

нет

да

2 Контролируется ли доступ?

Доступ фактически ограничен для всех, кто таким правом не наделен

нет

да

Предоставление

определенному кругу, согласие по ст.10.1 не нужно, нужно основание по ст.6

Распространение

неопределенному кругу, режим ст.10.1, обычно согласие по приказу РКН № 18

КАК КВАЛИФИЦИРУЮТ

предоставление	Табличка с ФИО и должностью на двери кабинета (РКН, 28.01.2022)
предоставление	Площадка только для зарегистрированных пользователей (РКН, 22.07.2021)
не распространение	Внутренний портал работников с контролем доступа (РКН, 01.07.2026)
распространение	Сайт закрыт от индексации, страница доступна любому по ссылке
распространение	Утечка в открытый доступ: так экспертно, суды квалифицируют как неправомерную передачу
распространение	Каналы не сводятся к Интернету: стенды, рассылки, печатные издания

Трансграничная передача ПД: что это и куда

Два признака определения и целенаправленность, две оси оценки страны

Privacy Advocates

п.11 ст.3 152-ФЗ

Передача на территорию иностранного государства иностранному лицу. Экспертный подход добавляет целенаправленность.

Это ТПД

- зарубежные метрики и облака, резервные копии за рубежом
- документооборот с иностранной материнской компанией
- бронирование и билеты у иностранных компаний
- удаленный доступ иностранного подрядчика из-за рубежа

Не ТПД

- передача гражданину РФ за рубежом
- распространение неопределенному кругу
- сервис без доступа к данным
- собственный филиал без статуса юрлица (спорно, позиция РКН менялась)

	дружественные	недружественные
в перечне РКН	БАЗОВЫЙ РИСК **например, Армения, Азербайджан, Сербия, Турция, Аргентина, Мексика** старт сразу после уведомления	ПОВЫШЕННЫЙ **государства ЕС, Великобритания, Швейцария, Япония, Республика Корея** старт после уведомления, выше шанс межведомственного запрета
вне перечня	ПОВЫШЕННЫЙ **например, ОАЭ** старт по истечении 10 рабочих дней, нужен обзор права страны	МАКСИМАЛЬНЫЙ **например, США** старт по истечении 10 рабочих дней, запасной маршрут заранее

Перечень: приказ Роскомнадзора № 253 (88 государств, без Украины) с 30.10.2026 вместо № 128. Ось дружественности - распоряжение № 430-р

Десять типовых стратегий локализации после 01.07.2025

Полоса показывает пример вероятности санкции по калькулятору Privacy Advocates

Калькулятор локализации
скачать

Privacy Advocates

	СТРАТЕГИЯ	ПРИМЕР РИСКА
1	**Перенос ИСПД в РФ** вся система и базы в РФ, затраты максимальные	0%
2	**Переход на бумагу** отказ от автоматизированной обработки	1%
3	**Перенос БД в РФ** база в РФ, серверы приложений остаются за рубежом	4%
4	**Промежуточная БД в РФ** запись сначала в базу в РФ, затем передача в зарубежную по ст.12	8%
5	**Сервис передачи ПД** зарубежный сервис только передает данные российскому оператору	13%
6	**Отказ от статуса оператора** оператор - иностранное лицо, российская компания пользуется системой	24%
7	**Обезличивание или шифрование** за рубеж уходят обезличенные или зашифрованные данные	36%
8	**Параллельный сбор в РФ и за рубеж** запись сразу в российскую и зарубежную базы	56%
9	**Репликация БД в РФ** сбор за рубежом и копия в российской базе	64%
10	**Оставить как есть** сбор в зарубежную базу без изменений	81%

Выбор: привлекательность стратегии складывается из стоимости жизненного цикла и совокупного риска. Проценты даны для примера, вероятности задаются экспертно под каждую ИСПД

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
RSP-015	Согласие на распространение: состав и границы	14 Распространение
TPD-016	ТПД: порядок с 01.03.2023 и новеллы 2026 года	20 ТПД

03.4

Хранение и уничтожение

- Процессы обработки ПД в организации
- Сроки хранения ПД
- По истечении срока: пять операций
- Уничтожение ПД: способ, средство, подтверждение

Процессы обработки ПД в организации

100 микроцелей в 12 макроцелях: основа для согласий и уведомлений в Роскомнадзор

Privacy Advocates

ПЕРСОНАЛ

01 Подбор персонала
поиск и оценка соискателей, резерв

02 Управление персоналом
прием, адаптация, учет, увольнение

03 Вознаграждение персонала
зарплата, удержания, мотивация

04 Обеспечение продуктивности, развития и безопасности персонала
обучение, охрана труда, медосмотры

05 Поддержка и мотивация персонала
ДМС, льготы, корпоративные события

06 Обеспечение пространственной мобильности персонала
командировки, релокация, транспорт

ДЕЯТЕЛЬНОСТЬ ОРГАНИЗАЦИИ

07 Обеспечение безопасности деятельности
пропускной режим, защита от посягательств

08 Информационно-технологическое обеспечение деятельности
коммуникации, оборудование и ПО, ИБ

09 Обеспечение эффективности и устойчивости деятельности
управление, контроль, защита прав

10 Сопровождение и поддержка деятельности
договоры, расчеты, закупки

11 Совершенствование и развитие деятельности
маркетинг, платформы, анализ аудитории

12 Ведение основной деятельности
профильная деятельность по уставу

12 макроцелей **100** микроцелей

Каталог целей обработки ПД
privacy-advocates.ru/pd/katalog_celej

Актуальность: 15.11.2025

Сроки хранения ПД

От рабочих дней на реагирование до лет хранения по основаниям закона

Privacy Advocates

Реагирование

7 рабочих дней

если субъект подтвердил, что ПД получены незаконно или не нужны для заявленной цели

152-ФЗ ст.20 ч.3

10 рабочих дней

при выявлении неправомерной обработки, если невозможно обеспечить ее правомерность

152-ФЗ ст.21 ч.3

10+5 рабочих дней

по требованию субъекта о прекращении обработки ПД

152-ФЗ ст.21 ч.5.1

Прекращение обработки

30 дней

после достижения цели обработки, если иное не предусмотрено договором или законом

152-ФЗ ст.21 ч.4

30 дней

при отзыве согласия, если хранить ПД для целей обработки больше не нужно

152-ФЗ ст.21 ч.5

6 месяцев

хранение в блокированном виде, если нет возможности уничтожить ПД в срок

152-ФЗ ст.21 ч.6

Хранение по основаниям закона

3 года

исковая давность по договору, где субъект сторона или выгодоприобретатель

ГК РФ ст.196

5 лет

после отчетного года для первичных учетных и налоговых документов

402-ФЗ ст.29; НК РФ ст.23, ст.24

5+ лет

при условии прохождения теста Почему именно такие сроки?

обоснование оператора

! **Ориентир для документов: Перечень типовых управленческих архивных документов с указанием сроков их хранения (утв. приказом Росархива от 20.12.2019 № 236)**

По истечении срока: пять операций

Что прекращает обработку, а что лишь приостанавливает ее или меняет режим

Схема обезличивания
скачать

Privacy Advocates

ОПЕРАЦИЯ	ОБРАТИМОСТЬ	ОБРАБОТКА	НОРМА И ОРИЕНТИР
Уничтожение	необратимо	прекращена	п.8 ст.3, ч.7 ст.21 152-ФЗ: содержание не восстанавливается, факт подтверждается по приказу РКН № 179
Удаление	обратимо до перезаписи	не прекращена	не равно уничтожению: файловая система стирает указатель, данные восстановимы
Блокирование	обратимо	приостановлена	п.7 ст.3, ч.6 ст.21: до 6 месяцев при обоснованной невозможности уничтожить в срок
Архивирование	обратимо	до передачи в архив - в режиме 152-ФЗ	после оформленной передачи - вне 152-ФЗ (п.2 ч.2 ст.1), сроки по перечню Росархива
Обезличивание	обратимо	продолжается	п.9 ст.3, приказ РКН № 140: способ защиты, а не прекращения, обезличенные ПД остаются ПД

По достижении цели - уничтожение (ч.4 ст.21) либо обезличивание (ч.7 ст.5): коллизия законом не разрешена, РКН устно допускает обезличивание.

Уничтожение ПД: способ, средство, подтверждение

Необратимость и доказуемость проверяются отдельно

Privacy Advocates

1

Способ по носителю

- бумага: перекрестная резка, сжигание, вымарывание
- машинные носители: механическое уничтожение, стирание, сдача на утилизацию по описи
- SSD не затирают программной перезаписью, криптостирание в праве не закреплено

2

Средство защиты

- п.3.1 ч.2 ст.19 152-ФЗ: СЗИ с функцией уничтожения, прошедшие оценку соответствия
- форма оценки спорна: ФСТЭК допускает любую (04.10.2024), ФСБ - сертификацию (05.10.2024)
- невыполнение - ст.13.12 КоАП, а не ст.13.11

3

Подтверждение

- приказ РКН № 179: акт всегда, при автоматизированной обработке плюс выгрузка из журнала событий ИСПД
- хранить 3 года, электронный акт допустим
- при поручении сначала акт обработчика, затем оператора (РКН, 14.08.2026)

Ловушки

надзор с 2025 г. смотрит процесс, а не разовый факт

Резервные копии

выводятся из использования до ротации, восстановление из копии возвращает уничтоженное

Сохранившиеся данные

акт не спасает: рассылка после уничтожения ведет к штрафу по ч.5 ст.13.11

Забытые носители

ноутбуки, флешки, почта и выгрузки вне плана уничтожения

03.5

Система комплаенса

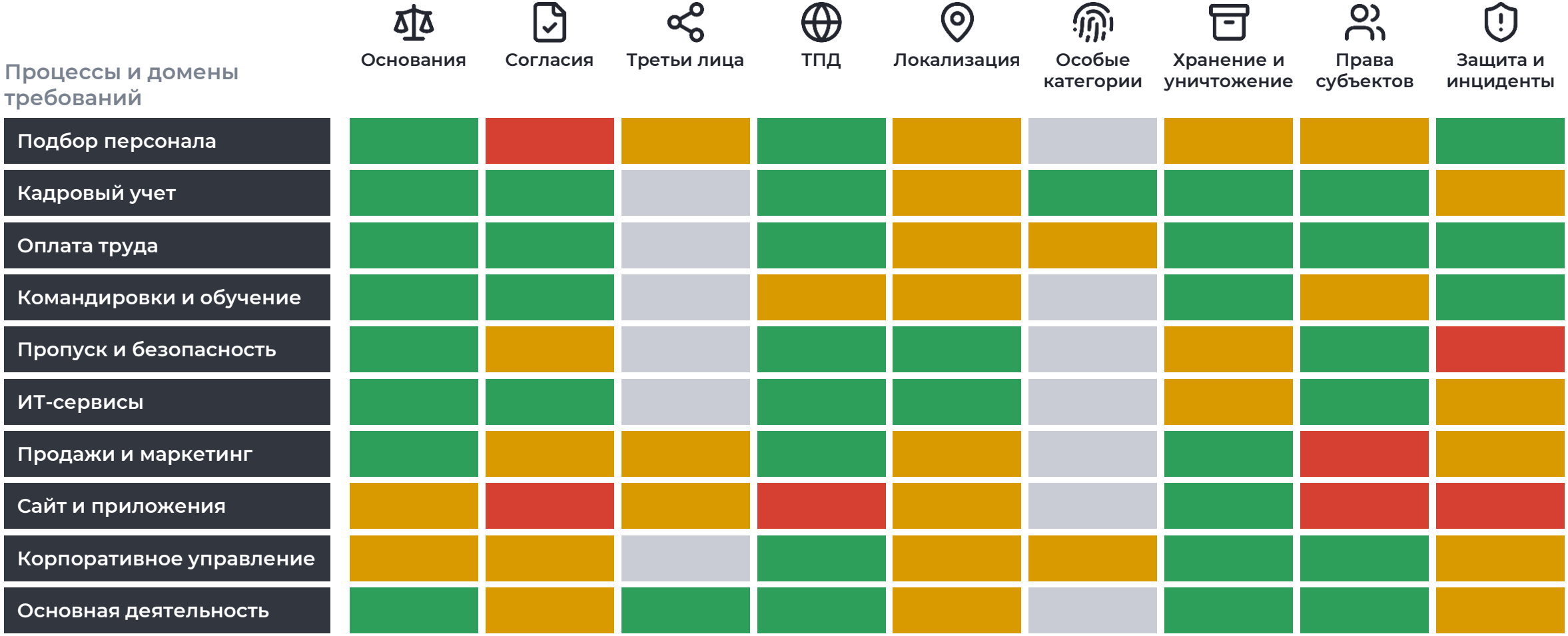
- Экспресс гэп-анализ процессов обработки ПД
- Проект privacy compliance: этапы и комплект
- Ответственный за организацию обработки ПД
- Риск-менеджмент обработки ПД

Экспресс гэп-анализ процессов обработки ПД

Разница между тем, как обработка сложилась, и тем, какой она должна быть по закону

Чек-лист ПД
скачать

Privacy Advocates



Каждая ячейка - оценка отклонения процесса по домену. По итогам строится план действий с приоритетами. **Пример, оценки условные.**

соответствует

незначительные отклонения

значительные отклонения

неприменимо

Проект privacy compliance: этапы и комплект

От обследования процессов к мерам ч.1 ст.18.1 152-ФЗ

Форма RoPA
скачать

Privacy Advocates

ЭТАП 1 Обследование

- сбор и анализ документов и сведений
- интервью, обследование процессов и ИСПД
- реестр наблюдений и реестр обработки (RoPA)

ЭТАП 2 Оценка и модели угроз

- перечень рекомендаций по итогам обследования
- оценка вреда субъектам (приказ РКН № 178)
- модели угроз и уровень защищенности (ПП-1119)

ЭТАП 3 Документы и решения

- политика, положение, приказы и формы
- уведомления РКН об обработке и о ТПД
- модель защиты, СЗПД и план мероприятий

Что запросит РКН при проверке: комплект по шести мерам ч.1 ст.18.1

- **Ответственный за организацию обработки**
- **Политика и локальные акты**
- **Меры безопасности по ст.19**
- **Внутренний контроль и аудит**
- **Оценка вреда субъектам**
- **Ознакомление и обучение**

Плюс документы по ПП-687 и подтверждение локализации. У ИП пп.1-2 не обязательны, у госорганов - перечень ПП-211. Проект листа (08.2026, 77 строк): уничтожение или обезличивание по достижении цели, критерии и обособление согласия, уведомление по целям.

Ответственный за организацию обработки ПД

ст.22.1 152-ФЗ: три функции как минимум, а не как потолок



Перечень ч.4 ст.22.1 примерный: три функции задают минимум, положение об ответственном с тремя пунктами закона роль недоописывает.

Один на оператора
в уведомлении указывается одно лицо, функционал делегируется внутри

Можно внешнего
работник другой организации или юрлицо, но внештатный ответственный дает низкую степень вреда по приказу № 178

Подотчетен исполнительному органу
право на сведения есть, гарантий независимости закон не дает

Не назначили
отдельного состава нет, должностным лицом отвечает руководитель. ИП и граждане назначать не обязаны

На практике шире
RoPA, экспертиза договоров, оценка вреда, инциденты, сопровождение проверок

С 2025 г. формальность дорога
оборотные штрафы, ст.272.1 УК, снижение штрафа через расходы на ИБ

Риск-менеджмент обработки ПД

Уровень риска = виктимность обработки × критичность отклонений

Калькулятор рисков
скачать

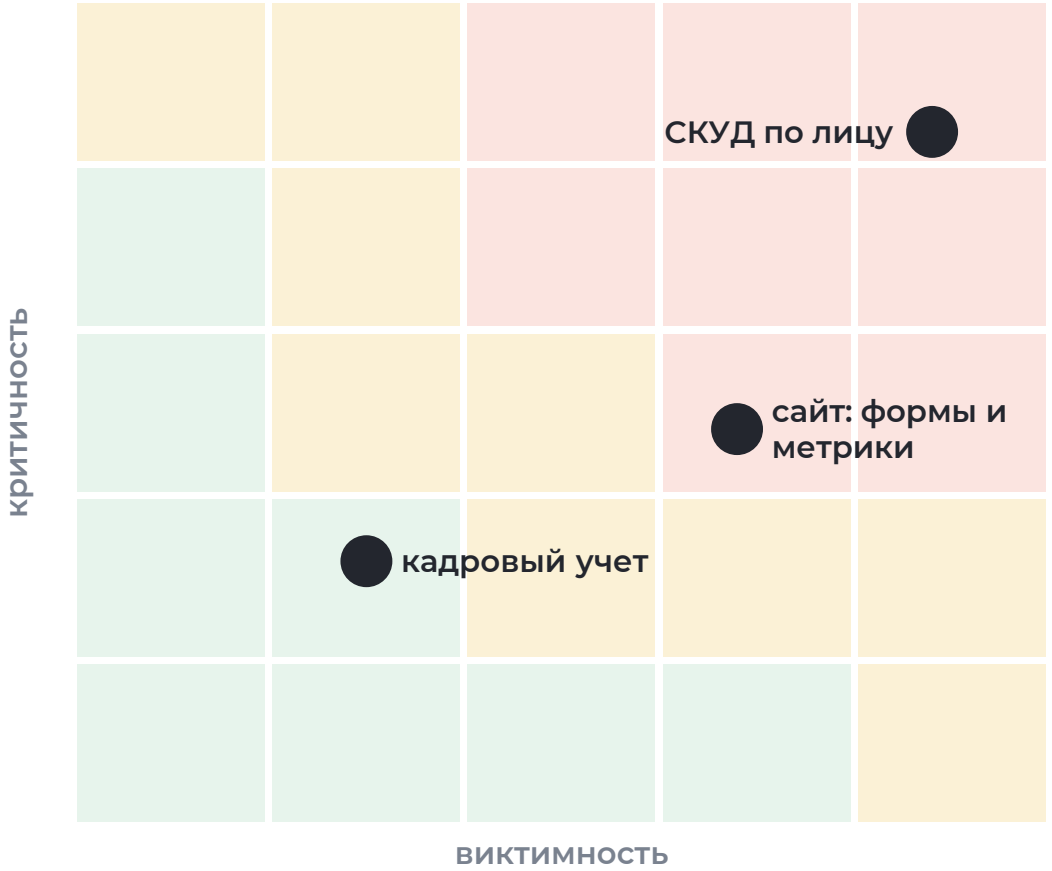
Privacy Advocates

Риск = Виктимность × Критичность

1. **Единица анализа**
   описать процесс и выбрать масштаб: от маркетинга целиком до отдельного сайта

2. **Виктимность**
   сумма 9 параметров (статус, цели, чувствительность, источники, субъекты, третьи лица, ТПД, масштаб, сценарии) × заметность от 1 до 4

3. **Критичность**
   взвешенная сумма по 10 доменам требований, жизненный цикл и безопасность весят до 4 баллов



Пороги под риск-аппетит: выше 200 высокий, 100-200 средний, ниже 100 низкий. Надзорная категория (ПП-1046 в ред. ПП-1286) считается иначе.

Не навреди	**Активное взаимодействие**	**Нет универсальной методики**	**Чем проще, тем лучше**	**Срок годности результата**	**Нет документов - нет риск-менеджмента**

Источники рисков

Три основных источника формируют 80% рисков в сфере ПД

Privacy Advocates

Дистанционный контроль РКН

Мониторинг сайтов, политик, форм согласий и cookie, сверка с реестром операторов без запросов и визитов

Жалобы субъектов

Обращения в РКН, прокуратуру и суд из-за непрошеных рассылок, навязанных согласий и запросов без ответа

Утечки ПД

Инциденты у оператора и его обработчиков. Уведомление РКН за 24 и 72 часа, оборотные штрафы за повторную утечку

80%

рисков

остальные 20% дают проверки РКН, конкуренты и бывшие работники

ДЛЯ ОПЕРАТОРА

Общие выводы

- Все три источника срабатывают извне, и момент выбирает не оператор
- Front-end compliance (сайт, политика, согласия, cookie) снимает претензии и РКН, и субъектов
- Ответ на запрос субъекта в течение 10 рабочих дней гасит жалобу до ее подачи
- План реагирования на инциденты и контроль обработчиков снижают цену утечки

Уведомление РКН об обработке ПД

ст.22 152-ФЗ, формы по приказу РКН № 180, подача через Портал ПД

Материалы РКН
скачать

Privacy Advocates

до начала

обработки

уведомление о намерении, по каждой цели (ч.3.1 ст.22)

30 дней

на внесение

в общедоступный реестр операторов, продление не предусмотрено

до 15-го

числа следующего месяца

уведомление об изменениях, только в части изменений

10 рабочих

дней

уведомление о прекращении, исключение из реестра за 30 дней

С 01.09.2022 ИСКЛЮЧЕНИЙ ТРИ

ч.2 ст.22 152-ФЗ

- **п.7** ГИС для защиты безопасности государства и общественного порядка
- **п.8** обработка исключительно без средств автоматизации
- **п.9** случаи законодательства о транспортной безопасности

Работники, договор с субъектом и общедоступные данные основаниями неподачи больше не являются.

ч.10 ст.13.11 КоАП с 2025 г.
юрлица 100-300 тыс. ₽, должностные лица госорганов и НКО 30-50 тыс. ₽, срок давности год

Индикатор риска
три и более расхождений уведомлений с политикой на сайте - основание внепланового мероприятия

ТПД отдельно
о трансграничной передаче подается самостоятельное уведомление по ст.12, в форме ст.22 только факт

Группа компаний
каждое юрлицо подает отдельно (РКН, 14.08.2026), старые уведомления актуализируют по форме № 180

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
FIN-001	Чек-лист из основных контролей обработки и защиты ПД	Ресурсы и контакты
DOP-002	Проект Положения об обработке и защите ПД в организации	06 Допустимость
SAJ-002	Диагностика комплаенса ПД на сайте	22 Сайт

03.6

Инциденты и ответственность

- Инцидент с ПД: квалификация и уведомления
- Оценка вреда и линия защиты по утечке
- Утечка ПД: лестница штрафов по ст.13.11 КоАП
- Ст.272.1 УК: незаконный оборот ПД

Инцидент с ПД: квалификация и уведомления

Два вопроса в первые часы, сроки 24 и 72 часа

Комментарий к 266-ФЗ
скачать

Privacy Advocates

1 **ПД вышли за периметр?**
стали доступны внешним лицам: публикация, личная почта работника, копирование посторонним

2 **Причина - компьютерная атака?**
или иное нарушение безопасности объекта информационной инфраструктуры

Роскомнадзор
ч.3.1 ст.21 152-ФЗ, приказ РКН № 187, Портал ПД
да на вопрос 1

ФСБ через ГосСОПКА
приказ ФСБ № 77: подключенные - в НКЦКИ, остальные - той же формой через РКН
да на оба вопроса

Банк России
ФинЦЕРТ: 24 часа, 3 часа при усиленном и стандартном уровне, отчет за 30 дней
финрынок

0 **выявление**
отсчет с момента выявления оператором, РКН или иным лицом, возможно и обработчиком. Часы календарные

24 ч **первичное уведомление**
что произошло, предполагаемые причины и вред, принятые меры, контакт представителя

72 ч **дополнительное уведомление**
результаты расследования: причины, вред, меры, лица, по вине которых произошел инцидент

1 р.д. **если 72 часа пропущены**
РКН требует результаты расследования, ответ за один рабочий день

Неуведомление - ч.11 ст.13.11 (1-3 млн ₽), сама утечка - чч.12-18. При утечке у обработчика уведомляет оператор.

Оценка вреда и линия защиты по утечке

Приказ РКН № 178 как документ, который работает в деле

Вред приватности
скачать

Privacy Advocates

Высокая	биометрия и спецкатегории вне случаев закона, ПД детей по договору с ними вне закона, обезличивание для исследований вне п.9 ч.1 ст.6, поручение иностранному лицу, сбор с БД за рубежом
Средняя	распространение на сайте оператора, обработка в дополнительных целях, маркетинг по базе от третьего лица, согласие через сервис без идентификации, согласие на несовместимые цели
Низкая	ведение общедоступных источников, внештатный ответственный за обработку

Акт: пять обязательных реквизитов, форма не утверждена, из нескольких степеней выбирается наивысшая. Порядок оценки оператор закрепляет локальным актом.

В деле об утечке акт подкрепляет довод о принятых мерах (экспертный вывод): ВС 21.01.2026 оставил штраф по ч.1 ст.13.11 министерству, не принявшему всех мер, включая внутренний контроль.

ЧЕТЫРЕ ОПОРЫ ЛИНИИ ЗАЩИТЫ

1. **Обстоятельства инцидента**
   масштаб, категории данных, длительность экспозиции, круг получателей
2. **Статус и поведение**
   впервые, признание, нет жалоб, устранение до протокола. Льгота МСП к чч.11-18 не применяется
3. **Меры до и во время**
   документы по ст.18.1 и 19, оценка вреда, внутренний контроль, работа защиты
4. **Действия после**
   уведомления в срок, оповещение субъектов, мониторинг копий, компенсации

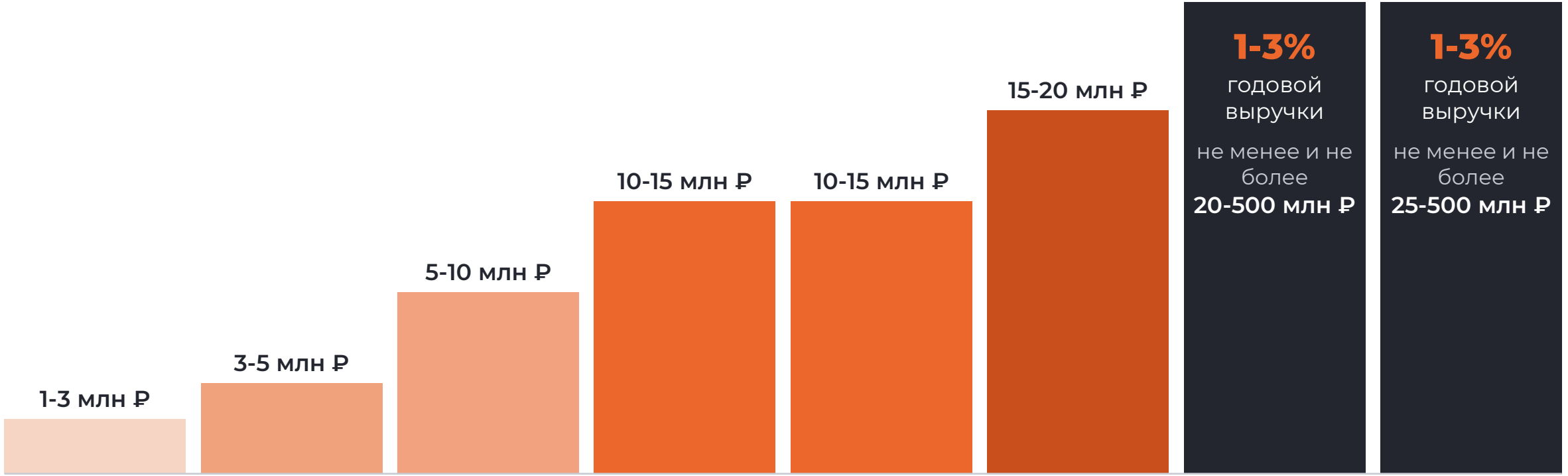
Дело РЖД (АС МО, 10.06.2026): РКН должен доказать, какие меры оператор мог, но не принял.

Утечка ПД: лестница штрафов по ст.13.11 КоАП

Редакция 420-ФЗ действует с 30.05.2025, штрафы для юридических лиц

Расчет оборотных штрафов
скачать

Privacy Advocates



ч.11	ч.12	ч.13	ч.14	ч.16	ч.17	ч.15	ч.18
нет уведомления за 24 или	1-10 тыс. субъектов или 10-100 тыс. ID	10-100 тыс. субъектов или 0,1-1 млн ID	более 100 тыс. субъектов или 1 млн ID	спецкатегории в любом объеме	биометрия в любом объеме	повторная утечка по чч.12-14	повторная по чч.16-17

Должностные лица госорганов и НКО: от 400-800 тыс. ₽ (ч.11) до 1,5-2 млн ₽ (ч.18), ИП отвечают как юрлица

Повторность держится год после исполнения постановления, следующая утечка стоит процент выручки

С 01.01.2026 дела снова у судов общей юрисдикции (508-ФЗ), скидка 50% при быстрой оплате не применяется

Ст.272.1 УК: незаконный оборот ПД

Действует с 11.12.2024 (421-ФЗ), отвечают только физические лица и только при умысле

Privacy Advocates

ПРЕДМЕТ: ТРИ ПРИЗНАКА СРАЗУ

Компьютерная информация
сведения в форме электрических сигналов (прим. к ст.272)

+

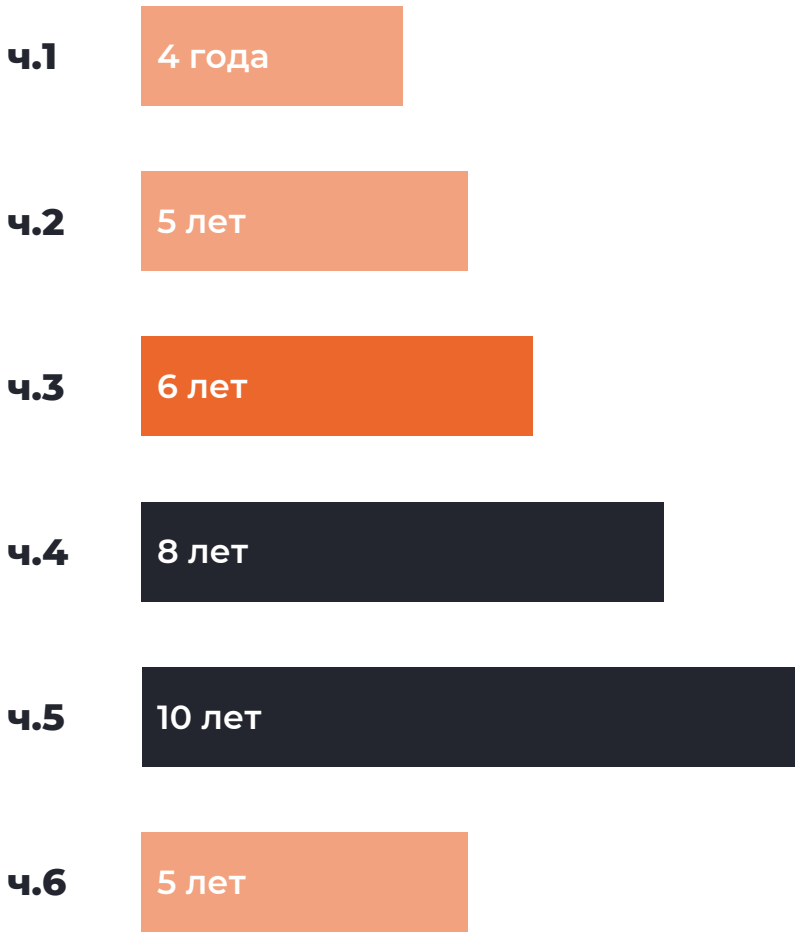
Содержит ПД
отнесение к ПД по п.1 ст.3 152-ФЗ

+

Получена незаконно
неправомерный доступ, вмешательство или иной незаконный путь

923 случая применения
за 10 месяцев 2025 г. (МВД). Типичные фигуранты - низовые звенья с доступом к базам, служебное положение вменяют и рядовым работникам продаж.

ЛИШЕНИЕ СВОБОДЫ, МАКСИМУМ



Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OTV-003	Ландшафт юридической ответственности за ПД	30 Ответственность
OTV-010	Смягчение по утечке: что работает, а что нет	30 Ответственность
OTV-016	Граница УК и КоАП при утечке	30 Ответственность

Обзор дает карту, а решения ищут в профильных разделах

Шесть выводов по жизненному циклу обработки и маршрут дальше

Privacy Advocates

Регулирование

обработка - любое действие с ПД. Цели и состав определяет оператор, обработчик действует по его поручению (п.2, 3 ст.3, ч.3 ст.6)

Основания

основание выбирают до сбора, согласие лишь одно из оснований ч.1 ст.6, письменная форма нужна только в случаях из закона

Движение данных

каждый поток квалифицируют: поручение или передача, распространение, ТПД. Локализацию по ч.5 ст.18 проверяют отдельно

Хранение

срок задает цель. По ее достижении ПД уничтожают или обезличивают (ч.7 ст.5), уничтожение подтверждают актом, а в ИСПД и выгрузкой из журнала

Система

комплаенс держится на ответственном (ст.22.1), политике, реестре и оценке вреда (ст.18.1), а уведомление Роскомнадзора подают до начала обработки (ч.1 ст.22)

Инциденты

об утечке уведомляют Роскомнадзор в течение 24 часов, о результатах расследования в течение 72 часов (ч.3.1 ст.21). Повторная крупная утечка ведет к оборотному штрафу (ч.15, 18 ст.13.11 КоАП)

Маршрут дальше: для своей организации пройдите навигатор по чек-листу ПД во входе Альманаха. Каждый пункт ведет в профильный раздел, а разделы 07 и 26 помогают выстроить систему и оценить риски

04

Осведомленность персонала

Что каждый работник делает с ПД и как защищает свои данные

04.1 Правила для работника

04.2 Мифы и полезные советы

04.3 Работник как субъект ПД

Раздел на сайте
privacy-advocates.ru/pd/trn

04.1

Правила для работника

- Четыре правила защиты ПД на рабочем месте
- Заметили инцидент с ПД - сразу сообщите
- Загрузка ПД в публичный ИИ-чат остается передачей данных
- Государство само ищет утечки ПД в сети

Четыре правила защиты ПД на рабочем месте

Что каждый работник делает каждый день

Privacy Advocates

Храните под замком

бумаги и флешки с ПД держите в отдельных шкафах, тумбах, сейфах или на отдельных полках

Чистый стол

не оставляйте документы с ПД на столе и сразу забирайте распечатки из принтера

Гости под присмотром

клиенты, поставщики и посетители находятся в помещениях с ПД только в сопровождении работников Компании

Правила ИБ

работая с ПД на компьютере, следуйте политикам и инструкциям Компании по информационной безопасности

Главное: защита ПД не порождает новых правил: достаточно соблюдать уже действующие правила защиты важной информации

Заметили инцидент с ПД - сразу сообщите

Что считать инцидентом и к кому идти: Роскомнадзор ждет уведомления в течение 24 часов

Privacy Advocates

Инцидент с ПД - любое нарушение конфиденциальности, целостности или доступности ПД, требований закона о ПД или соглашений об обработке ПД

ПРИМЕРЫ ИНЦИДЕНТОВ

- обработка без основания
- взлом учетной записи
- взлом системы или базы данных
- неправильное уничтожение файла
- неправильное уничтожение документа
- утеря устройства с ПД
- утеря документа с ПД
- письмо с ПД не тому адресату
- доступ к файлам без права
- публикация ПД без права
- передача ПД без права
- социальная инженерия

ЧТО ДЕЛАТЬ

Сообщить незамедлительно

- своему руководителю
- или любому руководителю отдела
- или ответственному за организацию обработки и защиты ПД
- подробности на внутреннем портале Компании

Осторожно: звонок "от руководства" о проверке утечки, а затем "от силовиков" - схема мошенников 2026 года по данным МВД. Пароли, коды и ПД по телефону и в мессенджерах не передают

Загрузка ПД в публичный ИИ-чат остается передачей данных

Решение суда и письмо Минпросвещения 2026 года, постановление КС 2017 года: что нельзя выносить в ИИ

Privacy Advocates

Отвечает компания

отправка работником чужих данных в личную почту, облако или внешний ИИ-сервис не освобождает оператора

Запрет по содержимому

в инструктаже запрещают не саму модель, а вынос сведений из перечня, с которым работник ознакомлен

Адрес сервиса

фактический получатель может не совпасть с известным брендом, адрес проверяют наравне с текстом

Минимум данных

перед вставкой убирают идентификаторы и сведения из перечня тайны, но очистка не снимает режим ПД и тайны

СУД ПЕРВОЙ ИНСТАНЦИИ, 26.05.2026

Увольнение за разглашение

пересылка на личный адрес и выгрузка документов в сторонний диалоговый сервис, выгрузка учтена среди обстоятельств без отдельной квалификации

ШКОЛЫ, 31.08.2026

Минпросвещения

рекомендует не загружать ПД учеников в ИИ-сервисы вне закрытого контура ГИС, в общедоступный сервис только с отдельного согласия родителя

Государство само ищет утечки ПД в сети

Минцифры в 2021 году заказало мониторинг открытых и закрытых источников, закупка № 0173100007521000114

Privacy Advocates

Где ищут

Открытые источники и darknet

- форумы киберкриминальной тематики, в том числе платные и закрытые
- Telegram-каналы и чаты киберкриминальной и ИТ-тематики
- блоги и сайты распространителей вредоносного ПО и вымогателей
- новостные ресурсы и комментарии пользователей
- форумы ИТ-тематики
- сервисы обмена текстом и кодом: Pastebin, GitHub

Что собирают

Сообщения об утечках

- о продаже ПД и баз ПД
- о покупке ПД и баз ПД
- любые другие сообщения о фактах утечки
- в фокусе - системы органов власти, операторов связи и госкомпаний с ПД граждан РФ

Вывод: срок уведомления Роскомнадзора об утечке идет с момента выявления, и неважно, кто ее нашел первым: Компания, регулятор или журналисты

С любым вопросом о ПД идите к ответственному

В Компании назначено лицо, ответственное за организацию обработки и защиты ПД

Privacy Advocates

Ответственный ведет **внутренний контроль** за соблюдением законодательства о ПД и помогает работникам. Обратитесь к нему незамедлительно, если вы

...видите угрозу своим правам

считаете, что при обработке ваших ПД в Компании нарушаются или могут быть нарушены ваши права и законные интересы

...заметили нарушение

обнаружили факт или угрозу нарушения действующих правил обработки и защиты ПД в Компании

...сомневаетесь

не уверены, правильно и законно ли поступаете вы или ваши коллеги при работе с ПД

Контакт: ФИО и e-mail ответственного лица Компании, а также ссылка на внутренний портал с правилами обработки ПД

04.2

Мифы и полезные советы

- Вредные советы: пять мифов о ПД
- Полезные советы: обращайтесь с чужими ПД как со своими

Вредные советы: пять мифов о ПД

Что говорят о ПД в курилке и как обстоит дело на самом деле

Privacy Advocates

ВРЕДНЫЙ СОВЕТ	КАК НА САМОМ ДЕЛЕ
Собирайте как можно больше данных, вдруг пригодятся	лишние данные - лишний риск: не становитесь складом данных и удаляйте ненужное. Утечка - вопрос не "если", а "когда"
Молчание - знак согласия	согласие дают активным действием так, чтобы его можно было подтвердить, например электронной подписью. Бездействие согласием не считается
Впишите рекламу в договор, клиенты потерпят	рекламные рассылки и звонки допустимы только с отдельного согласия (ст.15 152-ФЗ, письмо Банка России и ФАС от 06.09.2021 № ИН-06-59/70, АК/75514/21)
Для биометрии хватит согласия	с 01.06.2023 идентификация по лицу и голосу идет только через ЕБС, аутентификация через ЕБС или по ее векторам (572-ФЗ). Подумайте, нужна ли биометрия вообще
Иностранный сервис - не трансграничная передача	почти любая работа с ПД через иностранный сервис или с зарубежным партнером - ТПД. С 01.03.2023 о ней заранее уведомляют Роскомнадзор, и он вправе ее запретить

Полезные советы: обращайтесь с чужими ПД как со своими

Шесть правил, которые переводят принципы обработки на человеческий язык

Privacy Advocates

Данные принадлежат людям

вам их доверили на время, и ваши права на данные заканчиваются там, где начинаются права их владельцев

Берегите чужие ПД как свои

у всех есть секреты, и раз люди поделились ими с вами, храните их надежно

Говорите понятным языком

без "например, но не ограничиваясь" и без пустых целей вроде "для улучшения пользовательского опыта"

Новая цель - новое решение человека

хотите использовать данные иначе, дайте людям решить самим и заслужите их доверие или согласие

Не просите лишнего

если данные не нужны для услуги, не собирайте их

Предупредите о беде

если с данными что-то случилось и это может навредить людям, сообщите им раньше, чем они столкнутся с последствиями

Суть: это те же принципы законности, минимизации, прозрачности и честности, только без юридического языка

04.3

Работник как субъект ПД

- Наши права как субъектов не абсолютны
- Проверьте на Госуслугах, кто хранит вашу биометрию
- Ваши данные утекли: что делать и на что рассчитывать

Наши права как субъектов не абсолютны

У каждого права субъекта есть границы, и это не ошибка оператора

Privacy Advocates

Можно ли потребовать удалить любые свои данные?

Нет. Уточнения, блокирования или уничтожения требуют, если данные неполные, устаревшие, неточные, незаконно получены или не нужны для заявленной цели (ч.1 ст.14)

Прекратят ли обработку после отзыва согласия?

Не всегда: если есть иное основание из пп.2-11 ч.1 ст.6, например закон или договор, обработка продолжается (ч.2 ст.9)

Всегда ли откроют доступ к данным?

Доступ ограничивают, например, если он нарушает права других людей или обработка нужна для обороны, безопасности и правопорядка (ч.8 ст.14)

Исполнят ли требование прекратить обработку?

Да, за 10 рабочих дней с продлением на 5, кроме случаев пп.2-11 ч.1 ст.6 (ч.5.1 ст.21)

Помните: как в интерфейсе с надписью "Вы не можете удалить сами себя": право работает в границах закона, а отказ оператор обязан мотивировать со ссылкой на норму

Проверьте на Госуслугах, кто хранит вашу биометрию

Как увидеть, отозвать и удалить биометрию в ЕБС через личный профиль

Privacy Advocates

1. **Войдите в профиль**
   на Госуслугах откройте личный профиль
2. **Раздел "Биометрия"**
   видно, какая биометрия действует, кем и когда зарегистрирована
3. **Удалите ненужное**
   если биометрия чужая или не нужна, нажмите "Удалить"
4. **Проверьте согласия**
   в разделе "Согласия и доверенности" отзовите лишние согласия на биометрию

ТРИ УРОВНЯ БИОМЕТРИИ В ЕБС

УРОВЕНЬ	КАК ПОЯВЛЯЕТСЯ	ЧТО ДАЕТ
Упрощенная	приложение "Госуслуги Биометрия" или перенос из банка	ограниченный перечень услуг
Стандартная	приложение, загранпаспорт с чипом и телефон с NFC	ограниченный перечень услуг
Подтвержденная	очно в банке или центре обслуживания	все услуги, 5 лет

Право: отзыв по биометрии в ЕБС направляют оператору ЕБС через Госуслуги, а отказаться от сбора биометрии можно и через МФЦ (чч.14-16 ст.3 572-ФЗ)

Ваши данные утекли: что делать и на что рассчитывать

Практические шаги для работника как клиента банков и сервисов

Privacy Advocates

ЧТО УТЕКЛО	ЧТО ДЕЛАТЬ
ФИО, почта или телефон	риск кражи денег низкий, главное - никому не называть коды из SMS и другие данные
логины и пароли	сразу сменить пароль, а если он повторялся на других сайтах, сменить его везде
данные карт и счетов	обратиться в банк: обычно он узнает об утечке первым, а карту перевыпускают бесплатно
сканы документов	быть бдительнее к правдоподобным письмам и звонкам "из налоговой" о "долгах" и "штрафах"

КОМПЕНСАЦИЯ

Только через суд и небольшая

- отдельного механизма компенсаций за утечку нет
- в суде нужно доказать утечку у компании и свой вред
- по искам к Яндекс Еде суды снизили заявленные суммы до 5 000 ₽, кассация оставила это в силе (88-27523/2023)
- можно договориться с компанией напрямую о бонусах или скидках

Совет: проверить, есть ли ваша почта или телефон в известных утечках, можно в сервисе НКЦКИ chk.safe-surf.ru

05

Определение ПД

Где проходит граница ПД и как ее определять

- 05.1 Дефиниции и проблематика
- 05.2 Позиции РКН и практика
- 05.3 Источники, виды ПД и идентификация
- 05.4 Алгоритм определения и индекс атрибутивности



Раздел на сайте

privacy-advocates.ru/pd/opr

05.1

Дефиниции и проблематика

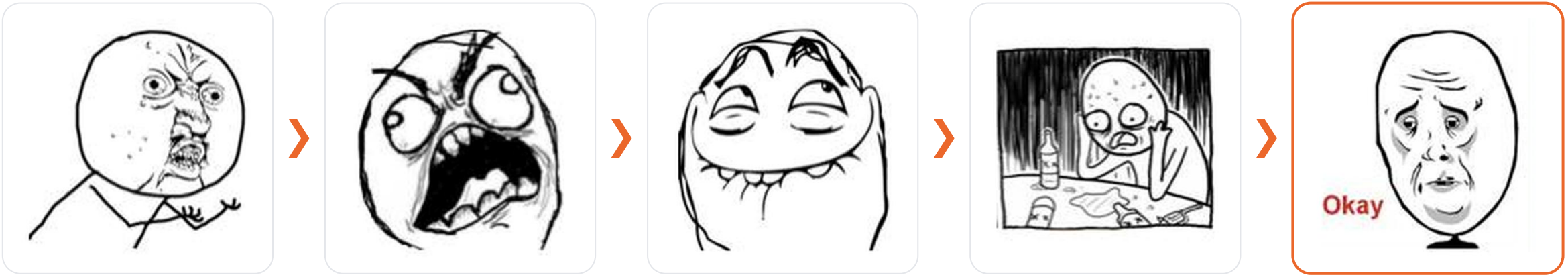
- Что есть ПД: пять стадий принятия неизбежного
- Дефиниция ПД и идентификатора
- Определение ПД широкое и не говорит, какой связи с лицом достаточно
- Суд ЕС считает лицо определяемым, если хватает разумных средств

Что есть ПД: пять стадий принятия неизбежного

Путь каждого, кто впервые всерьез читает определение персональных данных

Privacy Advocates

1 › 2 › 3 › 4 › 5



Отрицание

ПД - это только паспортные данные!

Гнев

Какой @#&$ придумал определение ПД?!

Торговля

ПД точно определяют конкретного человека

Депрессия

Все что угодно может быть ПД...

Принятие

Ну, хорошо, давайте разбираться

Дефиниция ПД и идентификатора

Три нормативных определения, на которых строится квалификация сведений

Privacy Advocates

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

п.1 ст.3 152-ФЗ О персональных данных



ИДЕНТИФИКАТОР

КоАП РФ

Уникальное обозначение сведений о физическом лице, содержащееся в информационной системе персональных данных оператора и относящееся к такому лицу

п.4 примечания к ст.13.11 КоАП РФ

Привязка к ИСПД оператора

VS

ИДЕНТИФИКАТОР

572-ФЗ

Уникальное обозначение сведений о лице, необходимое для определения такого лица

п.6 ст.2 572-ФЗ об идентификации и аутентификации с использованием биометрических ПД

Привязка к цели определения лица

Определение ПД широкое и не говорит, какой связи с лицом достаточно

Как в притче о слепых и слоне: каждый щупает свой признак, единого критерия нет

Privacy Advocates

01 Слишком широко

При буквальном толковании, которое правоприменение использует по умолчанию, к ПД можно отнести широкий круг сведений, в том числе выходящих за рамки разумно ожидаемого в данном контексте

02 Нет критерия связи

Дефиниция не говорит, какая связь сведений с прямой или косвенной определенностью либо определяемостью лица достаточна. Поэтому нет однозначного понимания, когда данные персональные, а когда нет

Следствие: спор о статусе данных ведется не о реквизите, а об элементе дефиниции, который оспаривается. Ответ дает квалификация по элементам в контексте, а не словарь реквизитов



Ориентиры практики по реквизитам, а не закрытый перечень

Суд ЕС считает лицо определяемым, если хватает разумных средств

Вероятностный и предположительный механизмы и сдвиг к относительному подходу

Privacy Advocates

2016

ВЕРОЯТНОСТНЫЙ МЕХАНИЗМ

Breyer, C-582/14

Динамический IP-адрес посетителя сайта ведомства ФРГ является ПД для оператора сайта, если у того есть законные средства получить недостающие сведения у интернет-провайдера. Учитываются средства, которые с разумной вероятностью могут быть использованы для объединения сведений

2022

ПРЕДПОЛОЖИТЕЛЬНЫЙ МЕХАНИЗМ

OT, C-184/20, Литва

Публикация имени супруга или партнера в декларации интересов служащего косвенно раскрывает сексуальную ориентацию и потому является обработкой специальной категории. Учитываются и сведения, которые раскрывают чувствительную информацию после дедукции или сопоставления

2025

ОТНОСИТЕЛЬНЫЙ ПОДХОД

EDPS v SRB, C-413/23 P

Псевдонимизированные данные остаются ПД для передающего, у которого есть ключ, и могут не быть ПД для получателя, который не способен снять защиту и связать их с лицом

Для РФ это ориентир, а не норма: в 152-ФЗ критерия разумно вероятных средств оператора и любого иного лица нет, подход GDPR используется как доктринальный ориентир

05.2

Позиции РКН и практика

- Матрица ПД 2014 года показала тупик закрытого перечня
- QR-код сам по себе не ПД, а считанные с него сведения ПД
- Критерий уникальности e-mail суды то применяют, то отвергают
- Неизменность и уникальность восходят к Idem и Ipse

Матрица ПД 2014 года показала тупик закрытого перечня

Рабочая группа Консультативного совета при Роскомнадзоре разложила реквизиты на три уровня

Privacy Advocates

УРОВЕНЬ 1

Идентифицируют сами по себе

- Серия и номер паспорта
- СНИЛС
- ИНН
- Биометрические данные
- Банковский счет и номер карты

Приоритет у идентификаторов, присваиваемых государством

УРОВЕНЬ 2

ПД с аспектом вероятного совпадения

ФИО + дата рождения + иная информация

место рождения, адрес, должность, семейное, социальное и имущественное положение, образование, контакты

ФИО или фамилия с инициалами + сведения, выделяющие лицо из ограниченного круга

объявление в подъезде о долгах жителя дома Иванова А.А.

УРОВЕНЬ 3

Не ПД по отдельности

- ФИО
- Адрес проживания
- Адрес e-mail
- Номер телефона
- Дата рождения

Табельный номер и иные идентификаторы - ПД только вместе с уровнем 1

Вывод: одни и те же реквизиты оказались и в ПД в совокупности, и в не-ПД по отдельности. Статус задают совокупность и контекст, поэтому каталог атрибутов - ориентир, а не закрытый перечень

QR-код сам по себе не ПД, а считанные с него сведения ПД

Две позиции Роскомнадзора 2021 года: о коде и о том, что за ним стоит

Privacy Advocates



Не ПД

Сам код

считывание



ПД

Считанные сведения

"...по представленным данным (QR-код) невозможно установить личность субъекта персональных данных, следовательно, данные персональными не являются"

Комментарий должностного лица Роскомнадзора, legalpress.ru/view/3195

Сведения, считываемые с QR-кода сертификата о вакцинации, относятся к ПД, но не к специальной категории. Их обрабатывают на общих основаниях, конфиденциально и уничтожают в течение 30 дней после достижения цели

Управление Роскомнадзора по ЦФО, письмо от 10.12.2021 № 112879-02-11/77

Логика одна: идентификатор объекта не становится идентификатором лица, пока нет информации, которая связывает его с конкретным человеком

Критерий уникальности e-mail суды то применяют, то отвергают

Роскомнадзор [2023]: неизменность и уникальность в совокупности относят данные к лицу

Privacy Advocates

ПОЗИЦИЯ РОСКОМНАДЗОРА: **Неизменность при присвоении** + **Уникальность** = **ПД конкретного лица**

Критерий применен

Ookla: e-mail сам по себе ПД

мировой судья уч. № 422 Таганского р-на г. Москвы, 12.07.2022; Второй КСОЮ оставил в силе 26.12.2022

Если для регистрации достаточно адреса почты, который нельзя использовать повторно, такой адрес - уникальный идентификатор пользователя и его ПД. Штраф за нарушение локализации 1 млн ₽ по ч.8 ст.13.11 КоАП, за повторное в 2023 году 6 млн ₽ по ч.9

Критерий отвергнут

СК Арсеналъ: без иных сведений не ПД

АС г. Москвы 20.10.2022, 9 ААС 11.01.2023, АС Московского округа 30.03.2023; ВС РФ отказал Роскомнадзору в передаче жалобы 21.07.2023

Абсолютной неизменностью адрес не обладает: после удаления ящика тот же адрес может получить новый пользователь, как и переданный другому абоненту номер телефона. Без дополнительных идентификаторов лицо по одному адресу не определить

Единства нет и внутри регулятора: в ответах 2022-2023 годов территориальные управления квалифицировали адрес по-разному. Статус мерцает в зависимости от контекста, инстанции и органа

Неизменность и уникальность восходят к Idem и Ipse

Философско-логическое обоснование свойств ПД и его предел

Privacy Advocates

IDEM

Тождество, структурный порядок

Тот же самый, а не другой: человек или предмет сохраняет тождество во времени и пространстве. Д. Парфит называет это numerical identity

P1 в момент t1 есть P2 в момент t2 тогда и только тогда, когда выполнен критерий K(P1(t1), P2(t2))



тождество лица во времени и среди других

IPSE

Самость, качественный порядок

Два предмета тождественны, если все свойства и отношения одного характеризуют и другой, и наоборот. Тождество возникает относительно инаковости: набор устойчивых качеств отличает человека от других

Предел аналогии: уникальность задается правилами конкретной системы идентификации, а не самим атрибутом. Уникальный реквизит еще не ПД, пока не установлена его связь с определяемым лицом

Суд не обязан соглашаться с Роскомнадзором, что сведения - ПД

Роскомнадзор [2024]: нет исключительного права определять ПД

Privacy Advocates

"Действующим законодательством Роскомнадзор... не наделен исключительным правом давать заключение о наличии или отсутствии в той или иной информации сведений, позволяющих по косвенным признакам определить субъекта персональных данных, то есть идентифицировать конкретное физическое лицо"

Постановление мирового судьи судебного участка № 44 района Орехово-Борисово Южное г. Москвы от 13.02.2024 по делу № 05-0010/44/2024, оставлено в силе решением Нагатинского районного суда г. Москвы от 03.04.2024 № 12-1747/2024

ФАБУЛА

Регулятор счел, что фамилия с инициалами и сведения об обращениях в госорганы позволяют определить заявителя. Суд не согласился и прекратил дело за отсутствием состава

СЛЕДСТВИЕ

1. Опора на разъяснение регулятора снижает риск административного спора, но не гарантирует исход судебного спора
2. Расхождение с позицией регулятора само по себе не делает позицию оператора неправомерной

Правоприменительная практика по определению ПД

От безусловных ПД до ПД только в совокупности с иными сведениями

Privacy Advocates

КАТЕГОРИЯ СВЕДЕНИЙ	КВАЛИФИКАЦИЯ	ПОЗИЦИЯ	ИСТОЧНИК
Фамилия и инициалы	В совокупности	Относятся к ПД, но без доп. сведений лицо не определяют: ФИО лишь сужает выборку	Нагатинский райсуд г. Москвы, 03.04.2024 № 12-1747/2024
Адрес электронной почты	В совокупности	Сам по себе ПД не является; становится ПД, если сведений достаточно для идентификации	Письмо Минцифры № П25-5623-ОГ; решения АС № А62-7498/2022 и № А40-139096/2022
Данные из трудового договора	ПД	Сведения о работнике, внесенные в трудовой договор, являются ПД	ВС Республики Саха (Якутия), 23.10.2013 № 33-4172/13
IP-адрес	Практика спорна	Указывает на устройство, но при сопоставлении с иными данными идентифицирует пользователя	13 ААС № 13АП-5614/2017; 8 ААС № 08АП-7948/2017
Табельный номер	ПД	Во взаимосвязи с другой информацией позволяет идентифицировать работника	Ответ РКН 05.04.2024 № 08-93449
Заработная плата	ПД	Относится к ПД работника	Роструд, вопрос № 96270 от 29.03.2018
Температура тела	ПД	Относится к ПД работника, например при проверке охранником на предприятии	Роструд, вопрос № 173408 от 16.12.2022
Категория годности к военной службе	Спецкатегория	В совокупности с иными идентифицирующими сведениями это специальная категория ПД	Минцифры, вопрос № 196072392 от 13.02.2024
Транспортные средства граждан	ПД	Сведения о ТС, зарегистрированных на физических лиц, относятся к ПД	4 ААС 02.08.2017 № 04АП-3856/17
Номер квартиры и долг за ЖКУ	Практика спорна	ВС РФ оставил в силе отказ в возбуждении дела, вопрос о ПД по существу не решал	Постановление ВС РФ 06.08.2025 № 46-АД25-13-К6

Мерцающие ПД

ВС РФ за пять месяцев оставил в силе противоположные оценки одних и тех же сведений

Privacy Advocates

ВЕРХОВНЫЙ СУД РФ

07.2023

НЕ ПД

Дело: *Роскомнадзор vs СК Арсеналъ*

Адрес электронной почты или номер телефона без иных сведений о человеке сами по себе не являются ПД

ВЕРХОВНЫЙ СУД РФ

12.2023

ПД

Дело: *ФАС vs 2gis.ru*

Адрес электронной почты сам по себе является ПД

Вывод: практику учитываем, но не абсолютизируем. Квалификация зависит от контекста обработки и совокупности сведений у оператора

Квантовые ПД: статус сведений зависит от наблюдателя

Аналогия с эффектом наблюдателя в опыте Юнга, хотя любая аналогия априори ложна

Квантовая механика
скачать

Privacy Advocates

	НЕТ НАБЛЮДАТЕЛЯ	ЕСТЬ НАБЛЮДАТЕЛЬ
Двухщелевой опыт эффект наблюдателя	 Электроны идут сразу через две щели как волны, на экране интерференция	 Детектор определяет щель, электроны ведут себя как частицы, на экране две полосы
Обработка данных эффект оператора	 Сведения остаются просто данными, пока никто не определяет по ним человека	 Оператор, заинтересованный в определении лица, превращает те же сведения в ПД

Вывод: информация становится ПД не абсолютно, а относительно наблюдателя, который заинтересован в определении человека

05.3

Источники, виды ПД и идентификация

- Каталог групп персональных данных
- Виды ПД по способам их получения
- Идентификация спрашивает "кто это?", аутентификация "ты ли это?"
- Закон и стандарты определяют идентификацию по-разному

Каталог групп персональных данных

15 групп и 186 записей: систематизация того, что на практике оказывается ПД

Privacy Advocates

Разделы каталога и число записей в них

1. Базовые идентифицирующие данные — 14
2. Личность и семья — 11
3. Образование и профессия — 9
4. Трудовая деятельность, воинский учет, госслужба — 26
5. Страхование, пенсия, налоги — 6
6. Поездки, транспорт, миграционный учет — 9
7. Деловая (экономическая) активность — 10
8. Сделки и реализация продукции — 10
9. Мероприятия, взаимодействия и спорт — 12
10. ИТ, связь и Интернет — 13
11. Геолокация и навигация — 2
12. Диагностика и телеметрия — 5
13. Медицинские данные — 15
14. (Псевдо)биометрия, геном и антропометрика — 33
15. Комплаенс, правоприменительные и особо чувствительные данные — 11

ПЕРСОНАЛЬНЫЕ ДАННЫЕ - ЭТО

≠ не только сведения, точно идентифицирующие конкретного человека

= **любые сведения, которые можно ассоциировать с человеком**

Каталог ПД

privacy-advocates.ru/pd/katalog_pd

Актуальность: 31.08.2026

Виды ПД по способам их получения

Восемь путей, которыми сведения о человеке оказываются у оператора

Privacy Advocates

Получены оператором извне

Предоставленные

получены от субъектов или их представителей

Например: заполнение веб-форм на сайте, представление резюме

Распространенные

взяты из общедоступных или открытых источников

Например: исследование учетных записей в социальных сетях

Наблюдаемые

зафиксированы путем отслеживания поведения субъектов

Например: онлайн-трекинг, геолокация, видеонаблюдение

Принятые

получены не от субъектов, а от других лиц

Например: рекомендация от бывшего работодателя соискателя

Созданы в ходе деятельности оператора

Инициированные

образованы путем совершения действий в отношении субъектов

Например: выплата зарплаты, угон личного автомобиля

Назначенные

временно или постоянно присвоены субъектам

Например: номер социального страхования, наименование должности

Производные

синтезированы после простого анализа других данных

Например: прибыльность клиента по числу посещений и покупок

Предполагаемые

спрогнозированы после продвинутого анализа наборов данных

Например: кредитный рейтинг, прогноз состояния здоровья

Идентификация спрашивает "кто это?", аутентификация "ты ли это?"

Разные процессы с разными алгоритмами: поиск 1-к-n и проверка 1-к-1

Privacy Advocates

	Идентификация [ID]	Аутентификация [AT]
Вопрос	**"Кто это?"**	**"Ты ли это?"**
Суть	установление личности путем установления сведений о лице	установление личности путем установления самого лица
Алгоритм	поиск и получение сведений о лице, как правило 1-к-n	проверка, подтверждение, верификация сведений о лице, как правило 1-к-1
Как устроено	лицо предъявляет уникальный идентификатор, сторона ищет сведения в своей базе или в базе третьей стороны	факторы знания (пароль, ПИН-код), владения (токен, смарт-карта), свойства (биометрия), один или несколько
Форма	автоматизированно или с участием уполномоченного лица, очно или дистанционно	
Биометрия	получение сведений о лице из ЕСИА и ЕБС, транзакционная модель	1-к-n или 1-к-1 в ЕСИА и ЕБС (транзакционная модель) или в КБС (векторная модель)

Авторизация - третий процесс: предоставление прав на определенные действия и проверка этих прав при попытке их совершить

Закон и стандарты определяют идентификацию по-разному

Дефиниции 572-ФЗ, 115-ФЗ и ГОСТов: от проверки сведений до сравнения идентификаторов

Privacy Advocates

ИДЕНТИФИКАЦИЯ

572-ФЗ, п.7 ст.2

совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с идентификатором

115-ФЗ, ст.3

совокупность мероприятий по установлению определенных законом сведений о клиентах, их представителях, выгодоприобретателях, бенефициарных владельцах и подтверждению достоверности этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий и (или) государственных и иных информационных систем

ГОСТ Р 58833-2020, п.3.24

действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов

АУТЕНТИФИКАЦИЯ

572-ФЗ, п.2 ст.2

совокупность мероприятий по проверке лица на принадлежность ему идентификаторов посредством сопоставления их со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификаторами посредством использования аутентифицирующих признаков в рамках процедуры аутентификации, в результате чего лицо считается установленным

ГОСТ Р 58833-2020, п.3.4

действия по проверке подлинности субъекта доступа и (или) объекта доступа, а также по проверке принадлежности субъекту доступа и (или) объекту доступа предъявленного идентификатора доступа и аутентификационной информации

Биометрия по ГОСТ ISO/IEC 2382-37-2016. Идентификация (п.37.08.02) - поиск по базе биометрических регистраций и возврат идентификаторов контрольного шаблона, связанного с одним индивидом. **Верификация (п.37.08.03)** - подтверждение биометрического заявления при сравнении

05.4

Алгоритм определения и индекс атрибутивности

- Определение ПД раскладывается на четыре проверяемых элемента
- Алгоритм определения ПД: принципы
- Алгоритм определения ПД: механика
- Индекс атрибутивности данных: описание и параметры

Определение ПД раскладывается на четыре проверяемых элемента

Взгляд прайвасиста: каждый элемент дефиниции и предел его толкования

Privacy Advocates

Любая информация — **относящаяся** — **к прямо или косвенно определенному или определяемому** — **физическому лицу**

ФОРМА

сведения, сообщения, данные в любой форме: текстовой, графической, звуковой

НОСИТЕЛЬ

любой носитель, бумажный или машинный, независимо от формы представления

СОДЕРЖАНИЕ

сведения по своей природе не могут не относиться к субъекту

ЦЕЛЬ

получить информацию о субъекте или воздействовать на него

РЕЗУЛЬТАТ

обработка затрагивает интересы субъекта независимо от содержания и цели

ОПРЕДЕЛЕННОСТЬ

сведения отделяют лицо от группы, в которую оно входит

ОПРЕДЕЛЯЕМОСТЬ

сведения дают разумную возможность такого отделения

СУБЪЕКТ ПД

права субъекта персональных данных принадлежат физическому лицу

⚠ Носитель ПД сам ПД не является

⚠ "Слишком расширительного" подхода к ПД быть не может, проблемы операторов решаются в рамках 152-ФЗ

⚠ Разумную возможность оценивают по времени, усилиям и средствам, которые вероятно и возможно могут быть использованы

⚠ Сведения, связанные с юрлицом, тоже могут быть ПД, например о его работниках

Алгоритм определения ПД: принципы

Три опоры, которые снимают большинство споров о квалификации сведений

Privacy Advocates

I

Любые сведения о человеке - это ПД, пока прямо не доказано обратное

Презумпция: при сомнении сведения обрабатываются в режиме ПД

II

Принимаем во внимание, но не абсолютизируем правоприменительную практику

Решения судов и разъяснения ведомств фрагментарны и противоречивы

III

Используем аналогию определения биометрических ПД в ст.11 152-ФЗ

Проверяем сведения по трем признакам из определения биометрических ПД

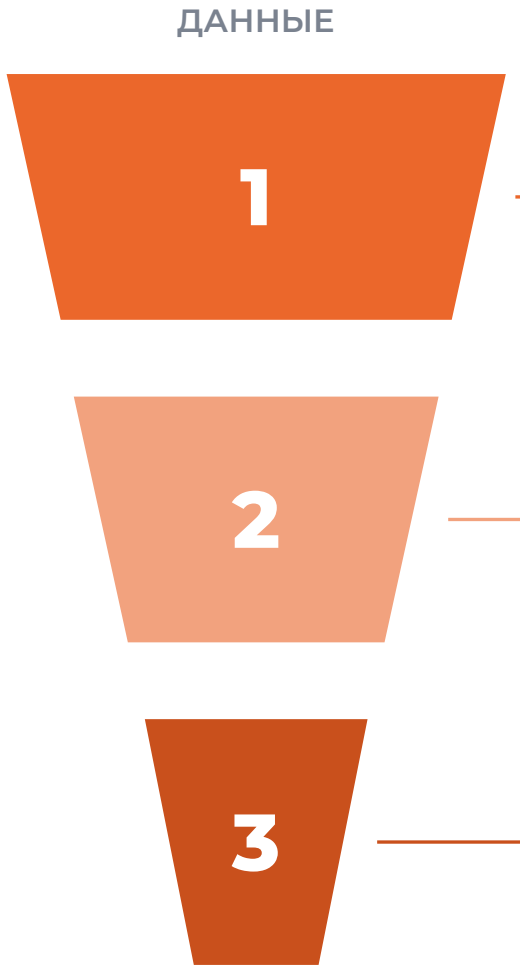
Ст.11 152-ФЗ: биометрические ПД - сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности

1. **Сведения о физиологических и биологических особенностях человека**
2. **Позволяют установить личность человека**
3. **Используются для установления личности человека**

Алгоритм определения ПД: механика

Три шага от сырых данных к выводу о целенаправленной обработке

Privacy Advocates



Выявляем полный состав данных в реальном, планируемом или возможном сценарии, включая идентификаторы: прямые и косвенные, постоянные и временные, сквозные и локальные, уникальные и повторяющиеся.

Диагностируем возможность **легального** определения человека оператором или иным заинтересованным лицом с учетом идентифицирующего потенциала данных: состава, структуры, взаимосвязей и источников.

Подтверждаем, что определение человека (или хотя бы его возможность) служит необходимым условием достижения цели обработки. Это и есть признак **целенаправленной обработки ПД**.

ЭКСПЕРТНЫЙ ПОДХОД

Целенаправленной обработки нет

- передача сведений оператором связи по каналам связи (транзит трафика)
- хранение в ЦОД при колокации или IaaS без доступа к содержимому
- формирование поискового индекса в сети Интернет
- хостинг модели ИИ без доступа к данным, с которыми она работает
- защита информации средствами СЗИ, пропускающими через себя трафик

Позиция регулятора строже. РКН считает участниками обработки (оператором или обработчиком по поручению) и ЦОД без доступа к данным, и транзитные платформы. Проект дорожной карты рынка ЦОД (август 2026 г.) предлагает освободить чистую инфраструктуру от ответственности за утечки, норма не принята.

Индекс атрибутивности данных: описание и параметры

Как оценить, насколько набор данных приближает к конкретному человеку

Privacy Advocates

Атрибутивность

свойство данных выступать признаком (характеристикой, атрибутом) человека

Индекс атрибутивности

оценка вероятности того, что совокупность данных позволит узнать (определить) конкретного человека и (или) уменьшить степень неизвестности в отношении него

Формула расчета

сумма свойств каждого типа данных в сценарии обработки (насколько они уникальны, неизменны и т.д.), умноженная на мультипликатор контекста: есть ли техническая возможность и юридическая цель связать данные с реальной личностью

Иначе говоря: свойства данных (их масса) умножаются на потребность в определении человека (контекст)

Индекс подводит итоговую черту в спорных ситуациях

Зеленая зона 33% и ниже

Обрабатываем данные, но не знаем людей. 152-ФЗ нас почти не касается

Желтая зона 34-66%

Не знаем имен, но можем вычислить человека или его устройство. Закон начинает применяться

Красная зона 67% и выше

Точно знаем, чьи ПД обрабатываем. Включаются все требования закона

Индекс атрибутивности данных: основные преимущества

Минимизация по расчету и защита, соразмерная контексту

Privacy Advocates

Data Minimization

Стимул к цифровой осознанности

Индекс работает как счетчик калорий

Каждое лишнее поле в базе данных, даже безобидное, увеличивает итоговый балл риска. Маркетинг и HR наглядно видят, что сбор данных про запас не бесплатен, а юридически дорог. Подход мотивирует удалять избыточные данные или снижать их атрибутивность, чтобы остаться в безопасной зеленой зоне.

Пример: вместо точного возраста указываем возрастной диапазон

Privacy by Design

Справедливость к контексту

Уникальность данных ≠ персональные данные

Индекс защищает бизнес от избыточных требований. Даже супер-уникальные идентификаторы (сложные хеши, GUID сессий), используемые только для техподдержки, а не для определения человека, дают низкий итоговый риск. Бюджет не уходит на защиту технических логов так же строго, как кадровой базы.

Пример: GUID сессии в логах техподдержки остается в зеленой зоне

Индекс атрибутивности данных

Формула и пример расчета

Калькулятор индекса
скачать

Privacy Advocates

ФОРМУЛА

1 Удельная атрибутивность

сумма баллов атрибута по семи характеристикам 1.1-1.7, по 1 или 2 балла, итого от 7 до 14

2 Индекс набора

сумма удельных атрибутивностей × мультипликатор контекста 2.1: определение человека необходимо 4, допустимо 2, исключено 1

3 Применимость 152-ФЗ

вероятность 1% + 99% × ln(И / мин) / ln(макс / мин), где мин = 7 × n и макс = 56 × n при n атрибутах

до 33%	34-66%	от 67%
маловероятна	вероятна	очевидна

ПРИМЕР РАСЧЕТА

Пользователь, представитель компании-клиента, заходит на сайт B2C-услуг и заполняет форму "Заказать консультацию"

Атрибут	1.1	1.2	1.3	1.4	1.5	1.6	1.7	Сумма
ФИО пользователя	1	2	2	1	1	1	2	**10**
Email корпоративный	2	2	2	1	2	1	2	**12**
Тема обращения	1	1	1	1	1	1	2	**8**
Динамический IP-адрес	2	1	1	1	2	1	1	**9**
Рекламный Cookie ID	2	1	1	1	1	1	1	**8**
User-Agent браузера	1	1	1	1	2	1	1	**8**

(10 + 12 + 8 + 9 + 8 + 8) × 4 = 220 **вероятность 80%, красная зона**

- **1.1** различающая способность
- **1.2** характер связанности
- **1.3** длительность связанности
- **1.4** степень изменчивости
- **1.5** сфера применимости
- **1.6** потенциал вреда
- **1.7** источник получения

выделены оценки в 2 балла

06

Допустимость обработки ПД

Риски, ответственность, сроки хранения и шесть базовых критериев допустимости

06.1 Рамка допустимости

06.2 Шесть критериев допустимости

Раздел на сайте
privacy-advocates.ru/pd/dop

06.1

Рамка допустимости

- Использование данных: выиграть или не проиграть?
- Проект Положения об обработке и защите ПД в организации

Использование данных: выиграть или не проиграть?

Две стратегии работы с данными и разная цена ошибки

Privacy Advocates

СТРАТЕГИЯ 1

Игра на победу

Максимизация выгоды



Данные как актив: больше сбора и аналитики, быстрее запуск продуктов

VS

СТРАТЕГИЯ 2

Игра на избегание неудач

Минимизация ущерба

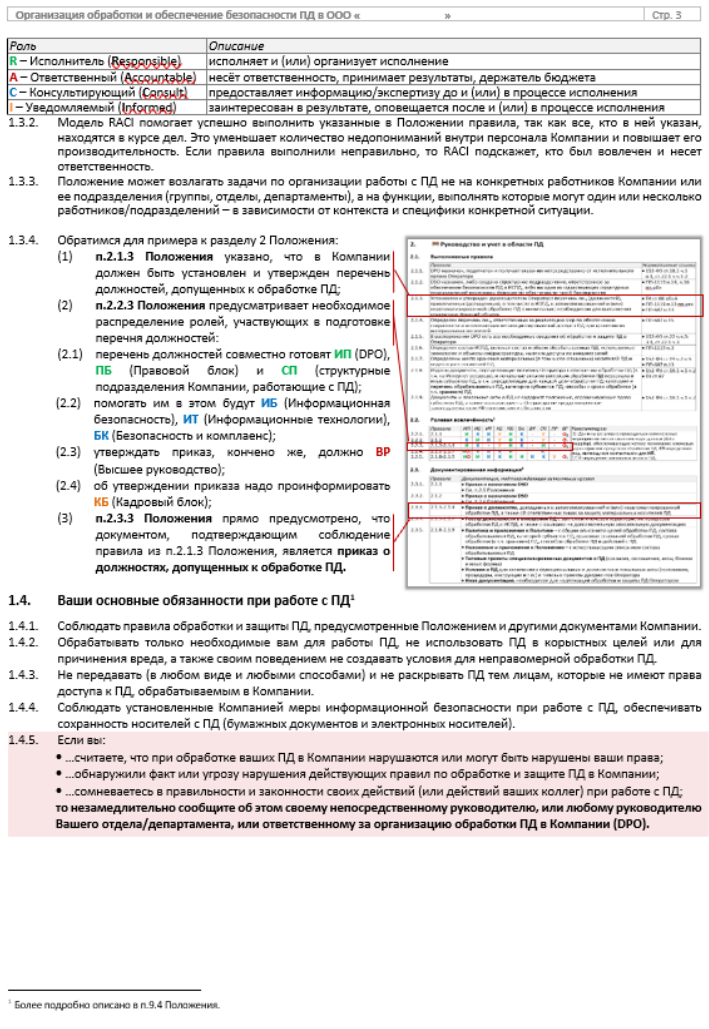


Данные как риск: меньше лишних данных, меньше поводов для претензий и штрафов

Проект Положения об обработке и защите ПД в организации

Демонстратор превращения чек-листа контролей в локальный нормативный акт

Privacy Advocates



Организация обработки и обеспечение безопасности ПД в ООО «» Стр. 3

Роль	Описание
R – Исполнитель (Responsible)	исполняет и (или) организует исполнение
A – Ответственный (Accountable)	несёт ответственность, принимает результаты, держатель бюджета
C – Консультирующий (Consult)	предоставляет информацию/экспертизу до и (или) в процессе исполнения
I – Уведомляемый (Informed)	заинтересован в результате, оповещается после и (или) в процессе исполнения

1.3.2. Модель RACI помогает успешно выполнить указанные в Положении правила, так как все, кто в ней указан, находятся в курсе дел. Это уменьшает количество недопониманий внутри персонала Компании и повышает его производительность. Если правила выполнили неправильно, то RACI подскажет, кто был вовлечен и несет ответственность.

1.3.3. Положение может возлагать задачи по организации работы с ПД не на конкретных работников Компании или ее подразделения (группы, отделы, департаменты), а на функции, выполнять которые могут один или несколько работников/подразделений – в зависимости от контекста и специфики конкретной ситуации.

1.3.4. Обратимся для примера к разделу 2 Положения:

(1) **п.2.1.3 Положения** указано, что в Компании должен быть установлен и утвержден перечень должностей, допущенных к обработке ПД;

(2) **п.2.2.3 Положения** предусматривает необходимое распределение ролей, участвующих в подготовке перечня должностей:

(2.1) перечень должностей совместно готовят **ИП** (DPO), **ПБ** (Правовой блок) и **СП** (структурные подразделения Компании, работающие с ПД);

(2.2) помогать им в этом будут **ИБ** (Информационная безопасность), **ИТ** (Информационные технологии), **БК** (Безопасность и комплаенс);

(2.3) утверждать приказ, конечно же, должно **ВР** (Высшее руководство);

(2.4) об утверждении приказа надо проинформировать **КБ** (Кадровый блок);

(3) **п.2.3.3 Положения** прямо предусмотрено, что документом, подтверждающим соблюдение правила из п.2.1.3 Положения, является **приказ о должностях, допущенных к обработке ПД.**

1.4. Ваши основные обязанности при работе с ПД[1]

1.4.1. Соблюдать правила обработки и защиты ПД, предусмотренные Положением и другими документами Компании.

1.4.2. Обрабатывать только необходимые вам для работы ПД, не использовать ПД в корыстных целей или для причинения вреда, а также своим поведением не создавать условия для неправомерной обработки ПД.

1.4.3. Не передавать (в любом виде и любыми способами) и не раскрывать ПД тем лицам, которые не имеют права доступа к ПД, обрабатываемым в Компании.

1.4.4. Соблюдать установленные Компанией меры информационной безопасности при работе с ПД, обеспечивать сохранность носителей с ПД (бумажных документов и электронных носителей).

1.4.5. Если вы:

- ...считаете, что при обработке ваших ПД в Компании нарушаются или могут быть нарушены ваши права;
- ...обнаружили факт или угрозу нарушения действующих правил по обработке и защите ПД в Компании;
- ...сомневаетесь в правильности и законности своих действий (или действий ваших коллег) при работе с ПД;

то незамедлительно сообщите об этом своему непосредственному руководителю, или любому руководителю Вашего отдела/департамента, или ответственному за организацию обработки ПД в Компании (DPO).

[1] Более подробно описано в п.9.4 Положения.

Материал состоит из трех частей

- Часто задаваемые вопросы — стр. 1
- Информационная брошюра — стр. 2-3
- **Текст проекта Положения** — стр. 4-33

Структура: 12 разделов

- **1** общие положения, роли, документы
- **2-11** области контроля, как в чек-листе ПД
- **12** термины и сокращения

В каждом разделе 2-11

- Соблюдаемые правила
- Ролевая вовлеченность (RACI)
- Документированная информация
- Связанные документы

Положение об обработке ПД

Скачать с Яндекс Диска

Актуальность: 31.03.2026

МОДЕЛЬ RACI

- **И** исполнитель
- **О** ответственный
- **К** консультирующий
- **У** уведомляемый

для 10 функций: от DPO и DSO до высшего руководства

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OTV-003	Ландшафт юридической ответственности за ПД	30 Ответственность
FIN-001	Чек-лист из основных контролей обработки и защиты ПД	Ресурсы и контакты

06.2

Шесть критериев допустимости

- Базовые критерии допустимости обработки ПД
- Предметность: ПД бывают в любой сфере жизни человека
- Целенаправленность
- Пропорциональность (целесообразность)

Базовые критерии допустимости обработки ПД

Шесть фильтров, через которые проходит любая обработка

Privacy Advocates

01 **Предметность** — 152-ФЗ ст.3 п.1

Любые сведения о человеке - это ПД, пока не доказано обратное

02 **Целенаправленность** — 152-ФЗ ст.5 ч.2

Конкретные, заранее определенные и законные цели

03 **Пропорциональность** — 152-ФЗ ст.5 ч.3-7

Минимум данных, раздельное хранение, без накопления впрок

04 **Легальность** — 152-ФЗ ст.6 ч.1

Каждая обработка опирается на основание из закона

05 **Транспарентность** — 152-ФЗ ст.14 ч.1-2

Субъект понимает, что и зачем делают с его данными

06 **Безопасность** — 152-ФЗ ст.7 и ст.19

Конфиденциальность ПД и меры по их защите



Предметность: ПД бывают в любой сфере жизни человека

П.1 ст.3 152-ФЗ: 15 групп сведений, которые относятся к человеку

Privacy Advocates

Любые сведения о человеке - это ПД, пока прямо не доказано обратное



ПД - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу

≠ **не только** точно идентифицирующая конкретного человека

= **но и** та, которую можно ассоциировать с человеком

Целенаправленность

152-ФЗ ст.5 ч.2

Privacy Advocates

Обработка ограничивается конкретными, заранее определенными и законными целями

- ✓ формулировка конкретна, без общих фраз вроде "осуществление прав и законных интересов оператора или третьих лиц" или "достижение общественно значимых целей"
- ✓ цель определена на этапе сбора ПД, а новая цель для ранее собранных ПД совместима с исходной
- ✓ цель законна: не нарушает установленные требования и не вступает с ними в противоречие

Необходимость обработки обоснована, если

- ✓ цель не может быть достигнута иным способом
- ✓ альтернативы без обработки ПД или с меньшим объемом ПД есть, но требуют несоразмерно больших затрат или усилий оператора



Пропорциональность (целесообразность)

152-ФЗ ст.5 ч.3-7

Privacy Advocates

- Минимизируется перечень собираемых и обрабатываемых ПД
- Раздельно хранятся категории ПД, в том числе несовместимые между собой по целям обработки
- Идентификаторы (ФИО, e-mail, телефон, адрес) и данные о взаимодействии (услуги, покупки, переписка) хранятся в разных базах
- Нет накопления ПД "на всякий случай" и профилирования клиентов без жизненной необходимости
- Меньше поручений обработки третьим лицам: ответственность остается у оператора, а контроль за мерами безопасности снижается



Новость Роскомнадзора
rkn.gov.ru/press/news/news74733.htm

Легальность

152-ФЗ ст.6 ч.1

Privacy Advocates

Основной квартет оснований обработки ПД

п.1 Согласие субъекта ПД

п.2 Функции, полномочия и обязанности оператора

п.5 Договор оператора с субъектом ПД

п.7 Права и законные интересы оператора или третьих лиц

Вспомогательные основания, а также пп.4, 10, 11

п.3	участие оператора в судопроизводстве
п.3.1	участие в исполнительном производстве
п.6	защита жизни, здоровья, жизненно важных интересов субъекта
п.8	массмедиа, журналистская, научная, литературная, творческая деятельность
п.9	статистическая и исследовательская деятельность

Когда ~~прилег постоять сидя~~ используешь несколько правовых оснований для одной и той же обработки персональных данных



Транспарентность

152-ФЗ ст.14 ч.1-2

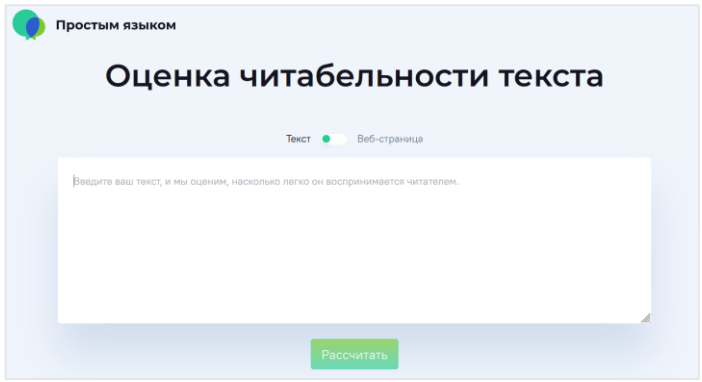
Privacy Advocates

Транспарентность = управление ожиданиями субъекта ПД → доверие субъекта ПД к оператору

Субъект ПД вправе получить информацию об обработке его ПД в доступной форме. **Контрольные вопросы для самопроверки оператора:**

? Был ли субъект надлежащим образом проинформирован об обработке ПД до ее начала или существенного изменения?

? Есть ли у субъекта разумное ожидание обработки ПД: логичное, справедливое и обоснованное с точки зрения обычного человека в конкретной ситуации?



5 формул понятности текста для русского языка

Flesch-Kincaid, Колман-Лиау, Automated Readability Index, SMOG, Дэйл-Чейл

Сервис: plainrussian.ru



Безопасность

152-ФЗ ст.7 и ст.19

Privacy Advocates

Классическая ИБ: 30+ подсистем, в том числе

- Идентификация и аутентификация
- Межсетевое экранирование и сегментация
- Анализ защищенности
- Защита от вредоносного ПО
- Защита каналов связи
- Криптографическая защита



Обезличивание

- Не является способом прекращения обработки ПД: обладает свойством обратимости
- Требования и методы обезличивания утверждаются Роскомнадзором

Обезличивание

Технологии защищенной обработки данных (ТЗОД)

- Обфускация: анонимизация и псевдонимизация, синтетические данные, дифференциальная приватность, доказательства с нулевым разглашением (ZKP)
- Обработка шифрованных данных: гомоморфное шифрование (HE), MPC, доверенные среды исполнения (TEE)
- Федеративное обучение (FL)

Белая книга ТЗОД

ЧАСТЬ

III

DPO и организация комплаенса

Кто отвечает за комплаенс, как он устроен и чем его автоматизировать

07 Организация комплаенса
08 Профессия прайвасиста
09 Автоматизация для DPO

07

Организация комплаенса

DPO, реестр обработки, политика и локальные акты

07.1 DPO и DSO

07.2 Реестр обработки и обследование

07.3 Политика и ЛНА

07.4 Внутренний контроль

Раздел на сайте
privacy-advocates.ru/pd/org

07.1

DPO и DSO

- Назначение ответственного подтверждают комплектом документов
- Три функции из закона - минимум для ответственного, а не предел
- Личную ответственность DPO определяют полномочия, а не приказ
- Ответственный за ПД может отвечать лично

Назначение ответственного подтверждают комплектом документов

Пять документов роли ответственного за организацию обработки и особенности внешней модели и группы компаний

Privacy Advocates

1

Приказ

факт и дата назначения со ссылкой на ст.22.1 и п.1 ч.1 ст.18.1 152-ФЗ, подпись назначенного

2

Инструкция

функции, право на сведения и распорядительные полномочия: Роскомнадзор на проверках и визитах просит ее вместе с приказом

3

Трудовые условия

соглашение об изменении функции (ст.72 ТК) либо согласие на дополнительную работу за доплату (ст.60.2, 151 ТК)

4

Доверенность

на ответы субъектам, письма в Роскомнадзор и участие в мероприятиях: без нее за письмо регулятору отвечал руководитель (дело № 12-392/2019)

5

Реестр операторов

в уведомлении одно лицо (п.7.1 ч.3 ст.22), при смене лица сведения обновляют (ч.7 ст.22)

ВНЕШНИЙ ОТВЕТСТВЕННЫЙ

Обязанности пишут в договоре прямо

а не отсылкой к закону: обязанности по ч.4 ст.22.1, передача сведений в объеме ч.3 ст.22, указания и отчетность перед исполнительным органом (ч.2 ст.22.1). В документах называют конкретное физическое лицо, иначе конструкцию рискуют оценить как ничтожную сделку или заемный труд

ГРУППА КОМПАНИЙ

Назначение в каждом юрлице

изъятий для групп нет: одно лицо может быть ответственным сразу в нескольких компаниях, но приказ издает каждый оператор, а сеть DPO по уровням группы, подгруппы и компании лишь координирует ответственных

Три функции из закона - минимум для ответственного, а не предел

Как ч.4 ст.22.1 152-ФЗ разворачивается в задачи, полномочия и следы, которые увидит проверяющий

Privacy Advocates

ФУНКЦИЯ	ЧТО ВХОДИТ НА ПРАКТИКЕ	ЧЕМ ПОДТВЕРЖДАЕТСЯ
Контроль	внутренний контроль соблюдения закона и требований к защите, ведение реестра обработки, экспертиза договоров, проектов и локальных актов	акты контроля, реестр наблюдений, заключения
Информирование	доведение требований до работников и обучение, перевод норм на язык рабочих правил	листы ознакомления, программа и журнал обучения
Коммуникации	прием и обработка обращений субъектов или контроль за ними, рабочий контакт из реестра операторов	журнал обращений, ответы в срок, замещающее лицо
Сверх минимума	оценка вреда, инциденты и уведомления, ответы органам и сопровождение проверок, мониторинг практики	положение о функции с полным набором задач
Полномочия	требовать выполнения требований, запрашивать информацию, предлагать изменения процессов и взыскания, давать поручения рабочей группе	должностная инструкция: по ней лицо квалифицируют по ст.2.4 КоАП

Независимость: закон дает прямую подотчетность исполнительному органу и безусловное право на сведения (ч.2, 3 ст.22.1), но не защищает от указаний по существу и увольнения, как ст.38 GDPR. Компенсируют это отчетностью первому лицу, метриками и требованиями даже к собственному подразделению

Личную ответственность DPO определяют полномочия, а не приказ

Критерий ст.2.4 КоАП, распределение ответственности внутри компании и граница уголовного риска

Privacy Advocates

КАК РАСПРЕДЕЛЯЕТСЯ ОТВЕТСТВЕННОСТЬ

Критерий ст.2.4 КоАП

должностное лицо выполняет организационно-распорядительные функции: решают инструкция и фактические полномочия, а не название роли

Решает владелец процесса

ответственный консультирует и рисков не принимает: оценку, согласование и решение фиксируют документом, иначе ответственность сместят на него

Нет назначения или полномочий - отвечает руководитель

ссылка на возложение функций на профильного специалиста руководителя не освобождает (дело № 7-81/2025 по ч.6 ст.13.12 КоАП)

Уголовный риск требует умысла

состав ст.272.1 УК умышленный (ст.25 УК), поэтому граница личного риска DPO проходит по его собственным действиям с данными, а не по должности

Полномочия опасны и без назначения

работника с распорядительными функциями и обработкой ПД привлекают и без назначения, а в деле № 4а-449/2017 даже рядового специалиста

Вывод: распорядительные полномочия, порядок согласования и фиксация решений определяют, кто ответит за нарушение, лучше любого приказа о назначении

Ответственный за ПД может отвечать лично

Роскомнадзор о статусе ответственного (DPO) и практика привлечения 2022-2025 годов

Privacy Advocates

ПИСЬМО ОТ 12.04.2023 № 08-31155

Ответ Роскомнадзора

на обращение А. Мунтяна о статусе ответственного за организацию обработки ПД

- оператор - юридическое лицо обязан назначить ответственного
- ответственным может быть работник, физическое лицо не работник или иное юридическое лицо
- назначать нескольких ответственных нельзя
- за нарушения отвечает оператор, а ответственность должностных лиц оценивают по обстоятельствам дела
- освобождение от ответственности решает только суд

ВОПРОСЫ, КОТОРЫЕ ОСТАЮТСЯ ОТКРЫТЫМИ

1. является ли внешний DPO, в том числе юрлицо, должностным лицом по КоАП
2. когда отвечает руководитель, а когда DPO вместо него
3. можно ли совместить работника и внешнего ответственного

РЕКОМЕНДАЦИЯ

Назначение оформляют приказом

в каждом юрлице группы свой ответственный, часть функций делегируют локальными актами

Практика: по обзору практики КоАП 2022-2025 годов (раздел 31) по ч.1-1.1 ст.13.11 из 106 наказанных должностных лиц 9 были DPO, по ч.2-2.1 - 2 из 19

DPO и DSO: две роли с разными источниками и надзором

Ответственный за организацию обработки и за безопасность в ИСПД: что различать при назначении

Privacy Advocates

ПРИЗНАК	DPO, СТ.22.1 152-ФЗ	DSO, П.14 ПП-1119
Когда обязателен	всегда для оператора - юридического лица	с 3 уровня защищенности, на 1 уровне еще и подразделение или функции подразделения (п.16)
Предмет	организация обработки: контроль, информирование, обращения	технический контур ст.19: угрозы, меры, доступ, регистрация действий, компьютерные инциденты
Кто проверяет	Роскомнадзор	ФСТЭК и ФСБ в государственных системах (ч.8 ст.19), у коммерческих операторов внепланово ФСБ и прокуратура
Санкция	ст.13.11 КоАП	ч.6 ст.13.12: юрлицу 50-100 тыс. ₽
Ценз	не задан, нужны право, процессы и ИТ	не задан; при СКЗИ - достаточные навыки (приказ ФСБ № 378), для значимых объектов КИИ - ценз приказа ФСТЭК № 235
Новое	с 2025 года формальное назначение дорого: оборотные штрафы и ст.272.1 УК	с 01.03.2026 в госсекторе приказ ФСТЭК № 117 действует наряду с ПП-1119

Совмещение: совмещение ролей Роскомнадзор допускает (вебинар 27.07.2023), но пробел одного контура назначением по другому не закрывается, а проверять собственные решения одно лицо не должно

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
BAZ-023	Ответственный за организацию обработки ПД	03 Обзор комплаенса
PRF-004	Пять принципов прайвасиста: бережно, по риску, без вреда	08 Профессия
SZP-003	Ответственному за безопасность ПД в ИСПД нужны полномочия	27 Защита и СЗПД

07.2

Реестр обработки и обследование

- Реестр обработки - ядро, из которого выводятся документы
- В реестре одна строка на цель, детали на связанных вкладках
- Все цели обработки ПД сводятся к 12 макроцелям
- Макроцель распадается на конкретные микроцели

Реестр обработки - ядро, из которого выводятся документы

Обязанности вести реестр в 152-ФЗ нет, но без него документы пишутся вслепую

Форма RoPA
скачать

Privacy Advocates

РЕЕСТР ОБРАБОТКИ ПД

Что, где, зачем и на каком основании

учетный документ по каждому процессу. В отличие от ст.30 GDPR закон его прямо не требует, и санкции за отсутствие нет

- надзорный запрос все равно собирает реестр заново: виды деятельности, категории субъектов и ПД, цели, основания, ИСПД с адресами баз
- ответ на мотивированный запрос обязателен (ст.20 152-ФЗ): по делу № А51-8682/2019 ВС РФ 16.10.2020 отказал в передаче жалобы оператора

Положение об обработке

по каждой цели категории ПД и субъектов, сроки и порядок уничтожения (п.2 ч.1 ст.18.1)

Уведомление в Роскомнадзор

с 01.09.2022 строится от целей так же, как реестр (ч.3.1 ст.22)

Оценка вреда и угрозы

чьи данные и в каких системах: вход для оценки вреда и модели угроз

Внутренний контроль

аудит сверяет факт с реестром, а расхождения и есть находки

Порядок: правку вносят сначала в реестр, затем в положение и при необходимости в уведомление. Тест простой: каждая цель уведомления и положения есть в реестре

В реестре одна строка на цель, детали на связанных вкладках

Состав записи, стартовая и зрелая форма и события, по которым реестр обновляют

Privacy Advocates

ЗАПИСЬ РЕЕСТРА: 11 ПОЛЕЙ НА КАЖДУЮ ЦЕЛЬ

1. процесс и подразделение-владелец
2. цель обработки
3. основание, по каждой операции свое
4. категории субъектов с отметкой о детях и уязвимых
5. категории и перечень ПД
6. операции с ПД
7. ИСПД и иные места хранения
8. получатели и обработчики
9. сроки обработки и хранения
10. порядок и способ уничтожения
11. меры защиты

СТАРТОВАЯ ФОРМА

Три вкладки

процессы, третьи лица, системы: из них уже выводятся положение и уведомление

ЗРЕЛАЯ ФОРМА

Еще шесть вкладок

бумажные собрания, управление комплаенсом, СЗПД, наблюдения, инциденты, история пересмотров

Когда обновлять

- новая цель или процесс
- новый состав данных
- смена получателей и обработчиков
- ввод или вывод ИСПД
- новые сроки и порядок уничтожения

Все цели обработки ПД сводятся к 12 макроцелям

Цель определяет основание, состав ПД, срок хранения и круг получателей

Privacy Advocates

- Подбор персонала
- Управление персоналом
- Вознаграждение персонала
- Обучение и развитие
- Мотивация и бенефиты
- Мобильность и релокация
- Безопасность деятельности
- ИТ-сервисы и защита информации
- Комплаенс и делопроизводство
- Договоры, расчеты и закупки
- Коммуникации, маркетинг и продажи
- Основная деятельность

Макроцель распадается на конкретные микроцели

Пример: макроцель "Подбор персонала" в перечне RPPA из 88 микроцелей

Privacy Advocates

88

ПЕРЕЧЕНЬ RPPA

Микроцелей в 12 группах

типовой набор целей для организации любого профиля

КАК ПОЛЬЗОВАТЬСЯ

Микроцель - единица учета

под каждую микроцель подбирают основание, состав ПД и срок хранения, а не под абстрактную цель "кадровая работа"

ПОДБОР ПЕРСОНАЛА: 8 МИКРОЦЕЛЕЙ

1. поиск соискателей на вакантные должности
2. информационное взаимодействие с соискателями
3. оценка соответствия требованиям, проверка знаний и способностей, опросы
4. проверка благонадежности: юридические, репутационные и комплаенс-риски, конфликт интересов, коррупция, достоверность сведений
5. решение о приеме либо отказе
6. преддоговорное взаимодействие (пребординг)
7. управление эффективностью подбора, включая удовлетворенность соискателей
8. формирование и ведение кадрового резерва

Итог обследования - реестр наблюдений, а не отчет в стол

Четыре этапа аудита соответствия, около трех месяцев на компанию, и как ранжировать находки

Privacy Advocates

1

Подготовка

сайт, политика и формы согласий; установочная встреча; защищенный канал обмена, а не открытое облако

2

Сбор данных

документы по готовому перечню и интервью от открытых вопросов к типовым; итог - реестр обработки и вкладка наблюдений

3

Корректирующие меры

мера, срок и ответственный по каждому наблюдению в самом реестре, а не в переписке; выбирает владелец процесса

4

Документы

политика, положение, инструкции, акты оценки вреда и уровня защищенности, уведомления и план по незакрытому

ОСЬ 1

Критичность

- роль: оператор или обработчик
- заметность для регулятора и субъекта
- объем, третьи лица, чувствительность данных, ТПД
- **прямой состав КоАП**: ответственность сразу, без окна на исправление

ОСЬ 2

Сложность устранения

- правка документов и форм
- доработка ИТ-систем
- перестройка отношений с третьими лицами
- новый процесс или контроль

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
BAZ-021	Экспресс гэп-анализ процессов обработки ПД	03 Обзор комплаенса
BAZ-022	Проект privacy compliance: этапы и комплект	03 Обзор комплаенса
RSK-010	Алгоритм в три шага	26 Прайваси-риски

07.3

Политика и ЛНА

- Словом политика называют три разных документа
- Структуру ЛНА выбирают по зрелости, а не по шаблону
- Мера принята, если ее можно предъявить по запросу

Словом политика называют три разных документа

Общая политика, политика ресурса и положение об обработке: охват, адресат и типичная подмена

Privacy Advocates

ДОКУМЕНТ	НОРМА	ОХВАТ И АДРЕСАТ	ТИПИЧНАЯ ОШИБКА
Общая политика оператора	п.2 ч.1 и ч.2 ст.18.1	подход ко всей обработке, неограниченный доступ для любого лица	ее нет вовсе: есть только политика на сайте
Политика сайта или приложения	ч.2 ст.18.1	сбор через ресурс, ссылка на каждой странице сбора; одна политика на несколько сайтов допустима	чужая политика или согласие под видом политики
Положение об обработке	п.2 ч.1 ст.18.1, п.8 ст.86 ТК	вся обработка, включая кадры и бухгалтерию; работникам под роспись	выложено наружу целиком с перечнями должностей и помещений

ПО КАЖДОЙ ЦЕЛИ ПЯТЬ ЭЛЕМЕНТОВ, П.2 Ч.1 СТ.18.1

- категории и перечень ПД
- категории субъектов
- способы обработки
- сроки обработки и хранения
- порядок уничтожения

НЕ РАБОТАЕТ

- политика не основание обработки: основания дает только ч.1 ст.6
- рекомендации Роскомнадзора 2017 года после изменения ст.18.1 неприменимы (Роскомнадзор устно, 22.08.2025)

Структуру ЛНА выбирают по зрелости, а не по шаблону

Три уровня документарной структуры и комплект документов Privacy Advocates по группам

растут зрелость и масштаб оператора

01

малый бизнес

Базовый

одно положение, приказы о назначении и допуске, формы согласий и поручений, публикуемая политика

02

средний бизнес

Модульный

зонтичное положение и профильные акты: работники, обращения, уничтожение, инциденты, ТПД

03

крупные компании и группы

Продвинутый

12 разделов по 10 областям контроля, роли закреплены за функциями, плюс брошюра-навигатор

КОМПЛЕКТ PRIVACY ADVOCATES

- политика
- положение об обработке и безопасности
- условия о конфиденциальности в договорах
- соглашения DTA, DPA, рамочное
- формы согласий и разъяснений
- оценка вреда, обучение, проверки
- реестры, журналы, акты
- документы о ТПД
- приказы, акт УЗ, модель угроз, меры защиты

ПП-211: перечень ПП-211 для госорганов частному оператору служит ориентиром: по каждому пункту решают взять отдельным документом, влить в положение или исключить, и решение фиксируют письменно

Мера принята, если ее можно предъявить по запросу

Ч.4 ст.18.1 152-ФЗ возлагает подтверждение мер на оператора: жизненный цикл документа от приказа до пересмотра

Privacy Advocates

1. **Утвердить приказом с датой**
   неутвержденный проект мерой не является, а дата файла реквизитом не служит

2. **Ознакомить под роспись**
   лист привязан к редакции; дистанционных знакомят на портале, только если это закреплено в договоре или ЛНА (ч.5 ст.312.3 ТК, дело № 88-16944/2020)

3. **Проверить на ограничения**
   нельзя сужать права субъекта и присваивать оператору полномочия: обращение только лично, отзыв согласия не ранее срока

4. **Сверять с политикой и реестром**
   расхождение ЛНА и политики Роскомнадзор называл типичным нарушением; спор решают по реестру

5. **Пересматривать**
   не реже раза в три года и по триггерам: блок инцидентов, оценка вреда, обособленное согласие

Ч.4 СТ.18.1 152-ФЗ

Подтверждает оператор

по запросу Роскомнадзора оператор представляет документы или иначе подтверждает меры. Вину в деле доказывает орган (ч.3 ст.1.5 КоАП), но непредставленное на практике считают непринятым

- по делу № А40-81171/2017 неразработка актов о ПД уволенных работников устояла в трех инстанциях (АС МО 15.01.2018)
- доказательства собирают двумя группами: рутина до инцидента и реагирование после

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
SAJ-010	Согласие отделяют от политики и пользовательского соглашения	22 Сайт
SAJ-012	Роскомнадзор: метрики включают после согласия, одной политики мало	22 Сайт

07.4

Внутренний контроль

- Внутренний контроль подтверждают утвержденный порядок и акт
- Аудит, оценка вреда и модель угроз друг друга не заменяют
- Аудит проверяет реальную обработку, а не только наличие документов

Внутренний контроль подтверждают утвержденный порядок и акт

Форму, состав и периодичность п.4 ч.1 ст.18.1 152-ФЗ отдает оператору: что ожидает увидеть регулятор

Privacy Advocates

Порядок

Постоянный локальный акт

- предмет: закон, требования к защите, политика и ЛНА оператора
- формат: внутренний контроль, внешний аудит или их сочетание
- методология: сверка с реестром, проверочный лист, интервью, обследование ИСПД
- **периодичность**: план раз в год или полгода и триггеры - жалоба, инцидент, смена процессов или закона
- проверяющие и их право на сведения

+

Акт

Результат конкретной проверки

- период, методология и проверяющие
- перечень проведенных мероприятий
- выявленные нарушения и нормы
- меры устранения, сроки и ответственные
- решения по результатам контроля

Практика: ВС РФ 21.01.2026 (№ 5-АД25-119-К2) оставил в силе штраф Минтруду 100 тыс. ₽ за утечку: в деле нет доказательств внутреннего контроля и аудита по ст.18.1, 19 и 22.1 152-ФЗ

Аудит, оценка вреда и модель угроз друг друга не заменяют

Четыре проверочные процедуры: норма, предмет, результат и как их истребует регулятор

Privacy Advocates

ПРОЦЕДУРА	НОРМА	ПРЕДМЕТ	РЕЗУЛЬТАТ	КАК ИСТРЕБУЮТ
Внутренний контроль и (или) аудит	п.4 ч.1 ст.18.1 152-ФЗ	соответствие обработки закону, политике и ЛНА	акт с нарушениями, мерами и сроками	отдельным пунктом запроса
Оценка вреда субъектам	п.5 ч.1 ст.18.1, приказ РКН № 178	возможный вред и соотношение с мерами	акт оценки вреда	отдельным пунктом запроса
Определение угроз	п.1 ч.2 ст.19, ПП-1119	технические сценарии для ИСПД	модель угроз или иной документ по выбору оператора	в документах о мерах безопасности
Оценка эффективности мер	п.4 ч.2 ст.19, п.17 ПП-1119, приказ ФСТЭК № 21	реализованные меры защиты, до ввода и не реже раза в 3 года	документ об оценке	в документах о мерах безопасности

Правило: аудит зонтичен: он проверяет, проведены ли оценка вреда и определение угроз, но их не заменяет, а техническую корректность мер проверяет специалист по ИБ

Аудит проверяет реальную обработку, а не только наличие документов

Комплексный подход по четырем срезам, выбор формата и пять типичных ошибок

Privacy Advocates

ЧЕТЫРЕ СКВОЗНЫХ СРЕЗА

срез 1

Данные и системы

какие ПД и в каких ИСПД обрабатываются

срез 2

Цели и принципы

минимизация, сроки, удаление по достижении цели

срез 3

Передачи

кому передают данные, включая обработчиков

срез 4

Доступы

кто и в каких ролях видит данные

ТИПИЧНЫЕ ОШИБКИ

- аудит на бумаге: порядок и акт есть, обследования нет
- лист вместо обследования: видно наличие политики, но не ее соответствие процессам
- хранение сверх сроков находит проверка, а не свой аудит (А40-81171/2017)
- аудит только по внешнему поводу: акты датированы жалобами и запросами
- акт без нарушений, сроков и проверяющих

Формат: свой регулярный контроль сочетают с внешним аудитом перед крупным запуском, после инцидента и перед визитом, но ответственность за меру остается на операторе

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
RSK-006	Оценка вреда и DPIA	26 Прайваси-риски
SZP-006	СЗПД собирают из мер, а средства подбирают под меры	27 Защита и СЗПД
FIN-001	Чек-лист из основных контролей обработки и защиты ПД	Ресурсы и контакты

Комплаенс держится на роли, реестре, документах и контроле

Выводы раздела

Privacy Advocates

01

Роль с полномочиями

ответственный обязателен для юрлица, но работает, только если у него есть инструкция, право на сведения и распорядительные функции

02

Реестр как единый источник

положение, уведомление, оценка вреда и аудит выводятся из реестра обработки, и любая правка начинается с него

03

Три политики, а не одна

общая политика, политика ресурса и внутреннее положение различаются охватом и адресатом, а не объемом

04

Документ предъявляем

мера существует, если введена приказом, доведена под роспись и находится по запросу (ч.4 ст.18.1)

05

Контроль по факту

аудит сверяет процессы с реестром и не подменяет оценку вреда и модель угроз

08

Профессия прайвасиста

Профессия, навыки и сертификация прайвасиста

08.1 Профессия и функции

08.2 Треки, навыки и роли

08.3 Privacy Tech

Раздел на сайте
privacy-advocates.ru/pd/prf

08.1

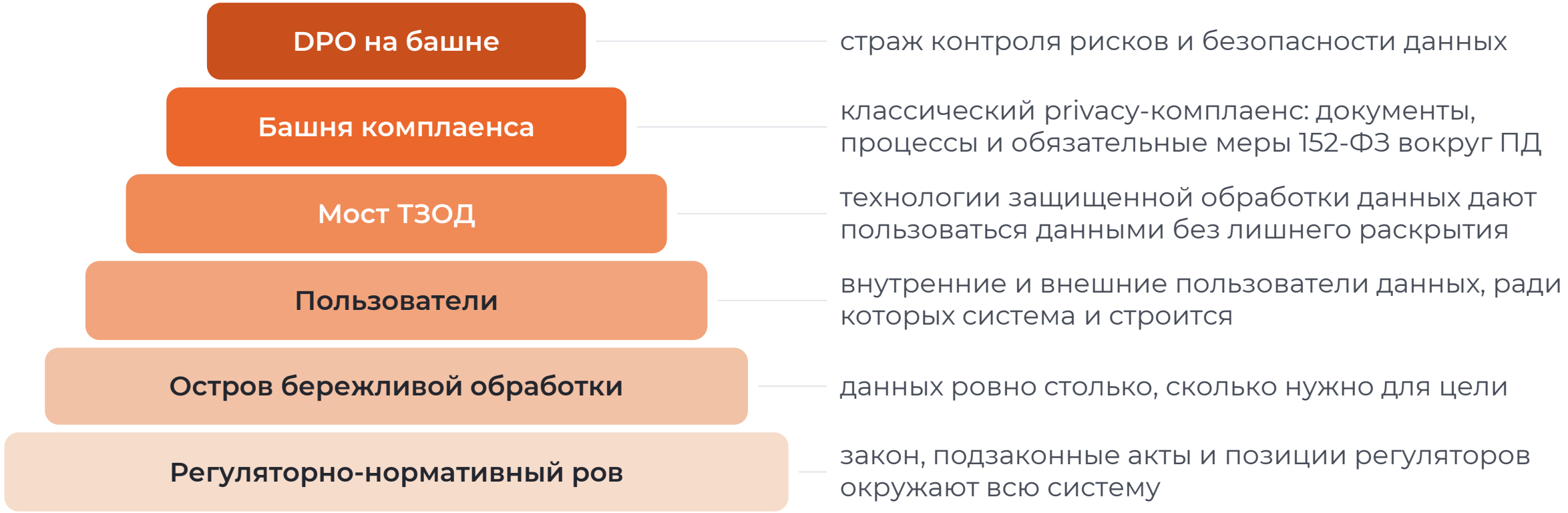
Профессия и функции

- Комплаенс ПД устроен как крепость с DPO на башне
- Прайвасист работает на стыке всех функций компании
- Проваленное задание в комплаенсе становится новым заданием
- Пять принципов прайвасиста: бережно, по риску, без вреда

Комплаенс ПД устроен как крепость с DPO на башне

Метафора системы комплаенса: ров регулирования, остров бережливой обработки, башня и мост

Privacy Advocates



Контекст: по доктринальной периодизации мировой комплаенс прошел три ступени: исполнение требований, privacy by design и конкуренция фреймворков. Российская модель ближе к первой: подотчетность через перечень мер ст.18.1 152-ФЗ

Прайвасист работает на стыке всех функций компании

С кем и с чем работает роль и что она дает каждой стороне

Privacy Advocates

ВНУТРЕННИЕ СТОРОНЫ

HR | IT | Legal | Compliance

ВНЕШНИЕ СТОРОНЫ

Регуляторы | Клиенты | Поставщики | Субъекты

ОБЪЕКТЫ РАБОТЫ

Люди | Процессы | Системы

СТОРОНА	ЧТО ДАЕТ ЕЙ ПРАЙВАСИСТ
Руководство	снимает неопределенность по требованиям и рискам, служит интерфейсом с регулятором и точкой входа в кризисе
Бизнес	переводит требования на язык рабочих правил, снижает затраты на соответствие, выявляет скрытые риски масштабирования
Смежные функции	профильный центр компетенций, который снимает с них нагрузку
Субъекты	прозрачность обработки и меньший риск нарушения прав
Регулятор	самостоятельной ценностью роль не является, но упрощает взаимодействие

Практика: ценность роли выглядит по-разному для каждой стороны, и от этого зависит язык разговора: руководству - риски, бизнесу - затраты и скорость, субъектам - прозрачность

Проваленное задание в комплаенсе становится новым заданием

Роль не заканчивается назначением: ее выстраивают по дорожной карте первых кварталов

Privacy Advocates

1. **Причина роли**
   инцидент, проверка, рост обращений, рекомендация аудиторов: от причины зависят ожидания
2. **Карта сторон**
   позиция, погруженность в ПД, вес в решениях и удобный канал каждого значимого лица
3. **Инвентаризация**
   документы, неписаные правила, следы процессов, прошлые инциденты, проверки и споры
4. **Три слоя требований**
   закон, лучшие практики и фреймворки ISO и NIST, собственные решения компании
5. **Точки интеграции**
   договоры, выдача доступов, проверки ИБ, архитектурный комитет, коммуникации, отчетность
6. **Быстрые победы**
   аудит сайтов, план реагирования на инциденты, читаемая политика, базовый реестр обработки

Метрика: успех первых месяцев измеряют закрытием наиболее значимых рисков, а не числом охваченных процессов и обученных работников

Пять принципов прайвасиста: бережно, по риску, без вреда

Принципы Privacy Advocates в работе с процессами нанимателя

Privacy Advocates

ПОЗИЦИЯ РОЛИ

Консультирует, а не решает

прайвасист не принимает решения об обработке и не запрещает: он предлагает варианты, обозначает риски и обеспечивает информированное решение владельца процесса.
Принять риск самому - значит создать конфликт интересов, как если бы архитектор здания взял на себя риск его обрушения

Привычка - вторая натура

бережное отношение к привычному для нанимателя способу ведения дел

Риск-ориентированный подход

обработка privacy-рисков с учетом риск-аппетита заинтересованных сторон

Не навреди

privacy-риски не снижаются за счет увеличения иных рисков

Активное взаимодействие

обсуждение предложений по обработке рисков с заинтересованными сторонами

Практичность результатов

итоговые материалы ориентированы на применение в операционной деятельности

Главная задача прайвасиста - консультировать бизнес

Опрос Sypher конца 2023 года, 120 специалистов по защите данных: доля выполняющих задачу среди всех респондентов

Privacy Advocates

93%

Консультации

по вопросам защиты данных, у штатных DPO 97%

89%

Уведомления

о конфиденциальности, у штатных DPO 92%

88%

Обучение

защите данных, у штатных DPO 94%

79%

Оценка воздействия

на конфиденциальность и защиту данных

ЗАДАЧА	ДОЛЯ	ЗАДАЧА	ДОЛЯ
Управление программами приватности	79%	**Создание и обновление реестра обработки ПД**	73%
Расследование инцидентов утечек	78%	**Оценка законных интересов организации**	73%
Соглашения об обработке (DPA) и договоры	78%	**Ответы на запросы субъектов ПД**	72%
Жалобы на нарушения приватности	78%	**Надзор за управлением согласиями**	64%
Отчетность руководству и аудиторам	76%	**Выявление и учет передач ПД в третьи страны**	64%
Политика хранения ПД	74%	**Оценка рисков поставщиков**	63%

Профессия сегментируется и уходит за пределы юриспруденции

Четыре тренда профессии и их проявления в 2025-2026 годах

Privacy Advocates

ДЛЯ РОССИИ

Цена формальной роли выросла

ответственный обязателен для любого оператора - юридического лица, а с 11.12.2024 действует ст.272.1 УК и с 30.05.2025 оборотные штрафы по ст.13.11 КоАП

- назначение на бумаге перестало быть дешевым решением
- размер оборотного штрафа связан с расходами на ИБ, ч.3.4-2 ст.4.1 КоАП

1. **Сегментация и специализация**

   роль делится на треки юриста, инженера, аналитика и менеджера программы. В группах компаний складывается сеть DPO по уровням группы, подгруппы и компании

2. **Не только комплаенс, но и дизайн-мышление**

   требования встраивают в процессы, продукты и системы на стадии замысла: правка замысла стоит обсуждения, а запущенного продукта - его остановки

3. **Упор на неюридические навыки**

   роли нужны три домена знаний: право, бизнес-процессы и устройство информационных систем. Назначение одного кадровика оставляет два домена без покрытия

4. **Рост сообщества**

   в отчет IAPP 2025-26 впервые вошли специалисты по AI governance, 77% из более чем 1600 респондентов из 60 стран имеют сертификат IAPP

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
TRE-001	Тренды законодательства о ПД в РФ	01 Тренды

08.2

Треки, навыки и роли

- Приватностью чаще всего руководят из юридической функции
- Навыки прайвасиста ведут от защиты данных к инновациям
- Девять навыков прайвасиста: от политик до дизайн-мышления
- Прайвасисту нужны этика данных и понимание бизнес-процессов

Приватностью чаще всего руководят из юридической функции

IAPP 2021: где находится руководитель приватности. IAPP 2025-26: медианные зарплаты по направлениям

Privacy Advocates

ПОДРАЗДЕЛЕНИЕ РУКОВОДИТЕЛЯ ПРИВАТНОСТИ

ФУНКЦИЯ	ВСЕГО	США	ЕС	БРИТ.
Юридическая	49%	58%	47%	42%
Регуляторный комплаенс	15%	13%	14%	18%
Информационная безопасность	6%	8%	6%	5%
ИТ	6%	5%	3%	6%
Корпоративная этика	4%	5%	4%	4%
Другое	13%	7%	17%	19%

МЕДИАННАЯ ЗАРПЛАТА 2025, ТЫС. $

НАПРАВЛЕНИЕ	МЕДИАНА
Технические роли AI governance в техсекторе	221,0
Юридические и комплаенс-роли в техсекторе	205,0
Приватность и AI governance вместе	169,7
Только AI governance	151,8
Только приватность	123,0

Тренд: у совмещающих приватность и AI governance медиана на 46,7 тыс. $ выше, чем у занятых только приватностью. Опрос 2025 года: более 1600 респондентов из 60 с лишним стран

Навыки прайвасиста ведут от защиты данных к инновациям

Девять профессиональных навыков на двух ступенях: сначала доверие, затем ценность данных

Privacy Advocates

СТУПЕНЬ 1

Защита данных

завоевать доверие клиента и двигаться в сторону подотчетности

1. управление защитой данных
2. управление ИТ-рисками
3. управление нарушениями безопасности
4. управление заинтересованными сторонами
5. аудит и комплаенс
6. управление данными

СТУПЕНЬ 2

Инновации на основе данных

использовать данные для создания новых или улучшенных товаров и услуг

1. этика данных
2. обмен данными
3. навыки дизайн-мышления

Контраргумент: тезис, что защита данных тормозит инновации, сравнительным опытом не подтверждается: КНР ужесточала режим защиты параллельно с выходом в лидеры разработки ИИ

Девять навыков прайвасиста: от политик до дизайн-мышления

Что стоит за каждым профессиональным навыком

Privacy Advocates

НАВЫК	СУТЬ
Управление защитой данных	политики и процедуры защиты ПД по применимому праву и лучшим практикам
Управление ИТ-рисками	прогноз и оценка ИТ-рисков для работы и прибыльности, стратегии снижения рисков обработки ПД
Управление нарушениями безопасности	выявление инцидентов и утечек, оценка обстоятельств и последствий, меры и коммуникации с заинтересованными лицами
Управление заинтересованными сторонами	ожидания и потребности стейкхолдеров с учетом требований и целей организации
Аудит и комплаенс	внешний и внутренний мониторинг и контроль, включая информирование о нарушениях и служебные расследования
Управление данными	правила обработки ПД на всех этапах жизненного цикла и рекомендации в сложных и неоднозначных контекстах
Этика данных	этические принципы при формировании процессов обработки ПД, см. раздел 02
Обмен данными	оценка ценности ПД для конкурентного преимущества и целей организации
Дизайн-мышление	путь от определения проблемы, исследования и идеи до реализации с вовлечением заинтересованных сторон

Прайвасисту нужны этика данных и понимание бизнес-процессов

Два ориентира: доклад WFA об этике данных и Науки об искусственном Герберта Саймона

Privacy Advocates

> Проектирует каждый, кто придумывает действия, чтобы превратить существующую ситуацию в предпочтительную

Герберт Саймон, Науки об искусственном (The Sciences of the Artificial), основа дизайн-мышления

ЭТИКА ДАННЫХ

1. WFA, Data Ethics: The Rise of Morality in Technology, июнь 2020
2. этика дает ответ там, где закон оценочен

БИЗНЕС-ПРОЦЕССЫ

1. требования встраивают в процессы, продукты и системы на стадии замысла
2. прайвасист проводит бизнес через варианты, а не запрещает

Прайвасист примеряет девять ролей

Ролевые модели: от архитектора видения до мыслителя, который оценивает и анализирует

Privacy Advocates

Архитектор

видение, миссия, ценности и ясность

Планировщик

краткосрочные и долгосрочные планы

Исполнитель

делает так, чтобы все случилось

Дирижер

объединяет усилия людей и открывает возможности

Учитель

наставник и коуч для команд

Хранитель

служит другим прежде себя

Новатор

генерирует идеи и создает условия для инноваций

Эксперт

понимает людей, бизнес и контекст, вплетает культуру и результат

Мыслитель

оценивает, анализирует и мыслит критически

08.3

Privacy Tech

- Privacy Tech делится на инструменты офиса приватности и компании

Privacy Tech делится на инструменты офиса приватности и компании

Классы решений по IAPP Privacy Tech Vendor Report 2022 и что спросить у поставщика

Privacy Advocates

ДЛЯ ОФИСА ПРИВАТНОСТИ: PRIVACY PROGRAM MANAGEMENT

- оценки воздействия и рисков
- управление согласиями
- карта данных
- запросы субъектов
- реагирование на инциденты
- мониторинг законодательства
- сканирование сайтов

ДЛЯ ВСЕЙ КОМПАНИИ: ENTERPRISE PRIVACY MANAGEMENT

- мониторинг активности
- поиск данных
- деидентификация и псевдонимизация
- корпоративные коммуникации

ИНСТРУМЕНТ САМ ОБРАБАТЫВАЕТ ПД

Три вопроса поставщику

- **где лежат мои данные**: поручение по ч.3 ст.6, локализация по ч.5 ст.18, ТПД по ст.12
- **откуда этот вывод**: прослеживаемость до нормы, позиции Роскомнадзора и практики
- **как я заберу все и уйду**: форматы выгрузки, возврат и уничтожение данных

Стоп-фактор: поручение и локализация - стоп-факторы: без них инструмент не проходит отбор при любой сумме баллов. Выбор инструментов подробно разобран в разделе 09

Прайвасист превращает обязательную роль в работающую функцию

Выводы раздела. В прайваси комплаенсе не бывает проблем, бывают приключения

Privacy Advocates

01

Роль обязательна, содержание - нет

ответственный нужен любому оператору - юридическому лицу, но три функции ч.4 ст.22.1 152-ФЗ - минимум, а не потолок

02

Независимость строят практикой

статусных гарантий, как у DPO по GDPR, в 152-ФЗ нет: их компенсируют отчетность первому лицу, метрики и право требовать

03

Консультирует, а не решает

прайвасист проводит бизнес через варианты и риски, решение и риск принимает владелец процесса

04

Междисциплинарность

право, бизнес-процессы и информационные системы плюс неюридические навыки и дизайн-мышление

05

Требования к лицу задают функции

ценза закон не устанавливает, Роскомнадзор отсылает к полномочиям по ч.4 ст.22.1 152-ФЗ (письмо от 03.05.2024 № 08-142784)

06

Метрики доказывают ценность

роль обосновывают закрытые риски и измеримые показатели, а не объем выполненной работы

09

Автоматизация для DPO

Как выбрать, проверить и не переплатить за обещания

09.1 Где автоматизация окупается

09.2 Как выбрать и проверить инструмент

09.3 Что ломается после внедрения

Раздел на сайте
privacy-advocates.ru/pd/atm

09.1

Где автоматизация окупается

- На что уходит время DPO
- Где автоматизация окупается
- Человек, ИИ или скрипт
- Семь классов инструментов

На что уходит время DPO

Рутина с жесткими сроками, где ошибка стоит денег

Privacy Advocates

СРОКИ, КОТОРЫЕ НЕЛЬЗЯ ПРОПУСТИТЬ

24 часа
Первичное уведомление РКН об инциденте с ПД
ч.3.1 ст.21 152-ФЗ

72 часа
Результаты внутреннего расследования инцидента
ч.3.1 ст.21 152-ФЗ

10 рабочих дней
Ответ на запрос субъекта или РКН, продление на 5 дней
ст.14 и 20 152-ФЗ

30 дней
Уничтожение ПД после достижения цели или отзыва согласия
ст.21 152-ФЗ, приказ РКН № 179

до 15 числа
Уведомление РКН об изменении сведений об обработке
ч.7 ст.22 152-ФЗ

до 500 млн ₽
оборотный штраф за повторную утечку с 30.05.2025, отвечает оператор, а не инструмент

Оговорка. Мы сами используем ИИ-ассистента по ПД, поэтому все критерии из презентации применяем и к своей работе

Где автоматизация окупается

Частота задачи и цена ошибки решают, сколько можно отдать инструменту

Privacy Advocates

Цена ошибки

высокая

низкая

Решает эксперт

Оценка вреда нового процесса

ТПД в новую страну

Ответ на запрос РКН

Готовит инструмент, решает DPO

Ответы на запросы субъектов

Уведомления РКН об инцидентах

Реестр процессов, акты уничтожения

Хватит шаблона

Разовые справки и письма

Редкие формы

Внутренние памятки

Полная автоматизация

Сроки и напоминания

Учет согласий и журналы

Мониторинг изменений регулирования

редко — **Частота задачи** — часто

Человек, ИИ или скрипт

У каждого шага задачи ровно один исполнитель, и он назначается заранее

Privacy Advocates

ПРИМЕР. ЗАПРОС СУБЪЕКТА О ЕГО ПД

Скрипт
Регистрация и отсчет 10 рабочих дней

→

Скрипт
Поиск записей субъекта по точным данным

→

ИИ
Разбор запроса и черновик ответа

→

Человек
Решение по спорному и подпись ответа

→

Скрипт
Отметка об отправке в журнале

ИСПОЛНИТЕЛЬ	ЧТО ДЕЛАЕТ И ЧЕМ ЗАДАЕТСЯ	ГДЕ У DPO
Скрипт автоматизация	**Без понимания текста.** Задается алгоритмом, входом, выходом и списком ложных срабатываний	Сроки, сверка реестра с перечнем систем, поиск по точному значению
ИИ-модель чтение и суждение	**Читает и рассуждает.** Задается инструкцией, критериями и запретами	Классификация обращения, признаки поручения в договоре, находка DLP в контексте
Человек DPO или владелец	**Решает в точках решения.** Получает сигнал с вариантами и последствиями, а остальная работа идет дальше	Квалификация инцидента, ТПД в новую страну, принятие остаточного риска

ПРАВИЛА РАСПРЕДЕЛЕНИЯ

1. Один шаг, один исполнитель
2. Смешанный шаг делится на два, скрипт отбирает кандидатов, ИИ их разбирает
3. Находка скрипта становится правкой без разбора, только если ответ однозначен
4. Любое изменение идет со страховочной копией и сверкой до и после

Семь классов инструментов

У каждого класса есть предел, о котором вендор обычно молчит

Privacy Advocates

Реестры процессов и ИСПД

Карта процессов, уведомления в РКН, учет обработчиков

Показывают то, что внесли, а не фактическую обработку

ИИ-ассистенты и правовые базы

Поиск норм и практики, черновики, разбор вопросов

Галлюцинации и додумывание, нужен свой тест

Конструкторы документов

Политики, согласия, поручения, ЛНА

Типовой текст не знает ваших целей и оснований



Запросы и инциденты

Сроки, маршрутизация, шаблоны ответов и уведомлений

Квалификацию инцидента и содержание ответа решает человек

Согласия и cookie

Сбор, учет и отзыв согласий на сайтах и в приложениях

По проекту Антифрод 3.0 сведения о согласиях пойдут в ЕСИА, вступление в силу с 01.03.2028

SGRC и ИБ-платформы

Риски, модели угроз, меры по ПП 1119 и приказу ФСТЭК № 21

Правовая часть комплаенса ПД обычно вторична

Поиск ПД в системах

Data discovery и DLP находят реальные копии ПД

Ложные срабатывания и долгая настройка под свои форматы

● что закрывает ● *где предел*

09.2

Как выбрать и проверить инструмент

- Восемь критериев оценки
- Инструмент сам обрабатывает ПД
- Пилот вместо демо
- ИИ-ассистента проверяют своим бенчмарком

Восемь критериев оценки

Оцениваем как подрядчика, которому передаем работу, но не ответственность

Privacy Advocates

	КРИТЕРИЙ	ВОПРОС ВЕНДОРУ	⚠ КРАСНЫЙ ФЛАГ
1	**Правовая актуальность**	Кто и за какой срок переносит изменения закона, где видна дата актуальности	Шаблоны без даты и автора, ссылки на утратившие силу нормы
2	**Прослеживаемость**	Можно ли от любого вывода перейти к норме, позиции РКН или судебному акту	Вывод без источника, черный ящик
3	**Инструмент как ИСПД** стоп-фактор	Где размещены данные, кто обработчик, какой уровень защищенности	Серверы или ИИ-модель за рубежом, нет поручения
4	**Доказательная сила**	Какие акты, журналы и отчеты дает система и примет ли их РКН	Дашборд вместо документа
5	**Встраиваемость**	Работают ли в системе владельцы процессов, есть ли интеграции с СЭД, HR и CRM	Системой пользуется только DPO
6	**Выход из системы**	В каком формате выгружаются реестры и журналы, что с данными после расторжения	Выгрузка только в PDF, данные заперты у вендора
7	**Полная стоимость**	Сколько стоят внедрение, наполнение, поддержка и время DPO	Цена по лицензии, наполнение ложится на вас
8	**Дорожная карта**	Как продукт отреагирует на изменения, например на проект платформы согласий в ЕСИА	Нет плана и истории обновлений

Каждый критерий от 0 до 2 баллов с весами под задачи компании. Стоп-фактор отменяет итог при любой сумме баллов

Инструмент сам обрабатывает ПД

Сервис, куда DPO загружает реестр и обращения, становится еще одной ИСПД

Privacy Advocates



1 Поручение обработки

ч.3 ст.6 152-ФЗ. Перечень действий, цели, конфиденциальность и требования к защите. Перед субъектом отвечаете вы

2 Локализация

ч.5 ст.18 152-ФЗ. При сборе ПД граждан РФ зарубежные базы данных не допускаются, в том числе у облачного сервиса

3 Защита

ПП 1119 и приказ ФСТЭК № 21. Уровень защищенности, модель угроз и меры, которые подтверждает вендор

4 Трансграничная передача

ст.12 152-ФЗ. Уведомление РКН до начала передачи и сведения о защите у зарубежного получателя

Стоп-фактор. Без поручения и локализации инструмент не проходит при любой сумме баллов, даже если он удобнее всех

Пилот вместо демо

Четыре шага проверки до подписания договора

Privacy Advocates

1. **Свои кейсы вместо демо**
   10-20 реальных кейсов компании, при необходимости обезличенных
2. **Ловушки с известным ответом**
   Утративший силу акт или согласие внутри договора, хотя с 01.09.2025 его оформляют отдельно
3. **Баллы и стоп-факторы**
   Каждый критерий от 0 до 2 с весами, размещение данных и поручение отсекают при любой сумме
4. **Письменное решение**
   Обоснование выбора пригодится при проверке, аудите и смене DPO

ТРИ ВОПРОСА ВЕНДОРУ



Где лежат мои данные?
локализация, поручение, ТПД



Откуда этот вывод?
прослеживаемость до нормы и практики



Как я заберу все и уйду?
выгрузка, форматы, удаление

ИИ-ассистента проверяют своим бенчмарком

Пять удачных ответов на демо ничего не доказывают

Privacy Advocates

250

вопросов из реальной практики DPO

50

диалогов по 5 вопросов проверяют удержание контекста

3

блока критериев на каждый вопрос вместо эталонного текста

Пример вопроса **Какие сроки уведомления РКН об утечке ПД?**

Обязательно	24 часа на первичное уведомление и 72 часа на результаты расследования, ч.3.1 ст.21 152-ФЗ
В идеале	Отсчет с момента выявления инцидента, состав сведений, ответственность за неуведомление по ч.11 ст.13.11 КоАП
Недопустимо	72 часа из GDPR как единственный ответ, смешение с уведомлением об обработке ПД, выдуманные размеры штрафов

Критерии, а не эталонный текст. Их легко поддерживать при изменении закона, а оценку можно повторять после каждого обновления сервиса

Отдельная категория. Аналитические вопросы о статистике дел и динамике позиции регулятора, где ошибку труднее заметить

Галлюцинация и конфабуляция

Стоп-условия считаются отдельно от баллов и обнуляют точность ответа

Privacy Advocates

Галлюцинация

ИИ выдумывает источник

- Несуществующая норма, письмо РКН или номер дела
- Ловится проверкой источника на существование
- Обнуляет точность ответа и идет отдельной метрикой

vs

Конфабуляция

опаснее

ИИ додумывает содержание

- Реальный акт с чужим содержанием или неверным исходом дела
- Проходит формальную сверку, ошибка спрятана в содержании
- Учитывается в стоп-пороге вместе с галлюцинациями

АС ЗСО, 14.05.2026, ДЕЛО № А27-7831/2025

50 000 ₽ штраф за жалобу с выдуманными и чужими актами, суд попутно отметил, что ИИ ответственности не снимает

Порог стоп-условий фиксируется до теста, а не подбирается под результат

Отказ тоже оценивается

Честное признание незнания лучше уверенной выдумки. Но систематические отказы там, где ответ в базе есть, говорят о проблеме поиска или модели, а не о пробеле в знаниях

РАЗДЕЛ 09. АВТОМАТИЗАЦИЯ ДЛЯ DPO

09.3

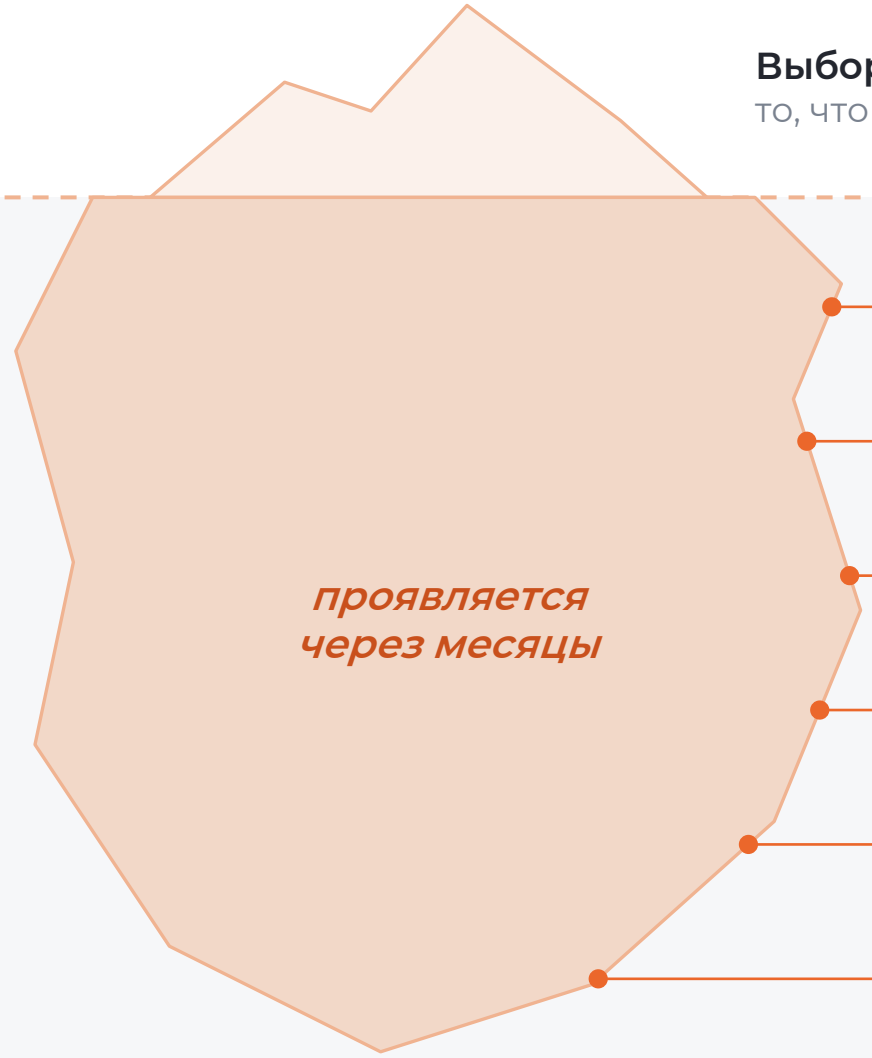
Что ломается после внедрения

- Что ломается после внедрения

Что ломается после внедрения

Покупка видна всем, провалы проявляются через несколько месяцев

Privacy Advocates



Выбор и демо
то, что обсуждают при покупке

подписание договора

1. **Реестр-фикция.** Заполнен из анкет без интервью, а РКН смотрит на фактическую обработку
2. **Зеленый дашборд.** Иллюзия соответствия убирает тему с повестки руководства
3. **Система только у DPO.** Новый проект, подрядчик или форма на сайте должны сами порождать задачу
4. **Шаблоны вместо мышления.** Согласия и политики выглядят верно, пока их не сверишь с целями
5. **Теневой ИИ.** Сотрудники уже загружают документы с ПД в публичные чат-боты, нужна легальная альтернатива
6. **Зависимость от вендора.** Проявляется при расторжении, поэтому план выхода пишется до подписания

Хороший инструмент тот, правоту которого вы можете доказать

ПЯТЬ ШАГОВ НА ПОНЕДЕЛЬНИК

- Выпишите десять самых частых задач и время, которое уходит на них за месяц
- Разложите их по матрице частоты и цены ошибки
- Для кандидатов на автоматизацию заполните карту из восьми критериев и задайте вендору три вопроса
- Проведите пилот на своих кейсах с ловушками
- Для ИИ-ассистента соберите свои 20-30 вопросов с критериями обязательно, в идеале и недопустимо

ЧАСТЬ

IV

Основания, права субъектов и особые категории

На каком основании обрабатывать ПД и какие данные требуют особого режима

10 Основания
11 ПД работников
12 ПД потребителей
13 Маркетинг и данные
14 Распространение ПД
15 Биометрические ПД
16 Генетические данные
17 Права субъектов

10

Правовые основания обработки

Согласие, договор, закон и законный интерес

10.1 Меню и выбор основания

10.2 Согласие и обособление

10.3 Договор и закон

10.4 Законный интерес

Раздел на сайте
privacy-advocates.ru/pd/osn

10.1

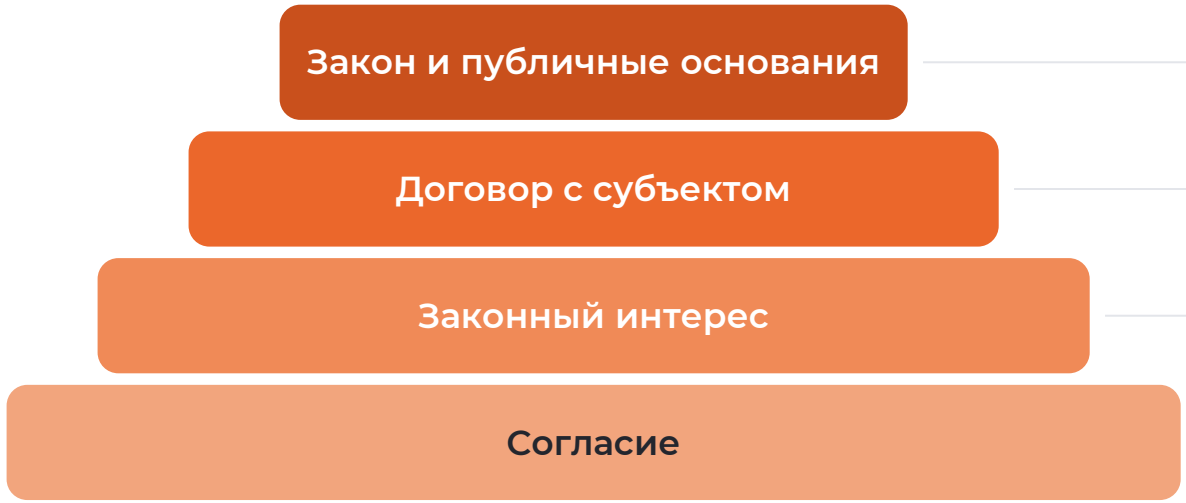
Меню и выбор основания

- Согласие проверяют последним, а не первым
- Если подходят два основания, выбирают одно по норме и фактам
- Основание выбирают по шагам и доказывают заранее

Согласие проверяют последним, а не первым

Обратная иерархия оснований: чем меньше обработка зависит от воли субъекта, тем она устойчивее

Privacy Advocates



включающий факт описан нормой, и от воли субъекта модель не зависит (пп.2-4, 11 ч.1 ст.6)

факт уже наступил и объем задан предметом, но отношения инициировал субъект (п.5)

связь с контекстом выстраивает сам оператор тестом цели, необходимости и баланса (п.7)

факт создают специально, и отзыв в любой момент отключает основание (п.1)

надежные

Закон, договор, раскрытие, суд

субъект не может их выключить, поэтому на них строят критичные и длящиеся процессы

пограничное

Законный интерес

законен, но оценочен, поэтому нужны письменная оценка и запасной сценарий

ненадежное

Согласие

отзывается в любой момент и остается для целей, у которых иного основания нет

Методология: закон основания не ранжирует, но Роскомнадзор видит согласие лишь вне случаев пп.2-11 ч.1 ст.6. Признак подмены простой: если отзыв согласия ничего в обработке не меняет, она держится на другом основании

Если подходят два основания, выбирают одно по норме и фактам

Шесть типовых развилок ч.1 ст.6 152-ФЗ и признаки, по которым на цель выбирают одно основание

Privacy Advocates

п.1 согласие | п.2 закон | п.4 госуслуга | п.5 договор | п.6 жизненно важные интересы | п.7 законный интерес

п.2	норма обязывает или управомочивает оператора	1	норма лишь предполагает обработку	п.7

Разграничение пп.2 и 7: Роскомнадзор, 27.07.2023. Пример: олимпиада школьников по ведомственному акту, п.2 (07.12.2023)

п.2	обязанность и полномочие	2	субъективное право с оценкой применимости	п.7

Пример: право акционера на документы общества

п.5	нужно для предмета договора	3	что не нужно для предмета, ищет собственное основание: договор интересом не достраивается	иное

Пример: рассылка, профилирование, скоринг по сторонним источникам

п.4	услуга начинается с запроса гражданина	4	функция не зависит от запроса	п.2

Пример: противоэпидемические меры по п.2, законного интереса у органа нет

п.6	только если согласие объективно невозможно	5	защита третьих лиц и общества	п.7

Пример: видеозапись конфликта для полиции

п.1	только если не подходит ни одно из пп.2-11	6	согласие не нужно и про запас не собирается (письмо Роскомнадзора от 03.10.2025)	пп.2-11

Пример: школа ведет журнал по пп.2, 4 после отзыва согласия родителем (Мосгорсуд, 2026)

Правило: сколько целей, столько оснований: доставка по договору, учет по закону, защита в суде по законному интересу, рассылка по согласию. Конкуренцию оснований Роскомнадзор устно допускает (14.08.2026), но запасное основание на ту же цель выдает непроработанную цель

Основание выбирают по шагам и доказывают заранее

Алгоритм подбора под процесс, журнал оснований и ошибки, которые всплывают при проверке

Privacy Advocates

1 **Цель и операция**
процесс с несколькими целями делят

2 **Категория данных**
для ст.10, 11 и 10.1 свои перечни

3 **Без согласия**
закон, суд, госуслуга, договор, раскрытие

4 **Законный интерес**
три критерия без обхода запретов

5 **Согласие**
если иного нет или его требует закон

6 **Фиксация**
политика, реестр, оценка, журналы

ЖУРНАЛ ОСНОВАНИЙ

Учет самих оснований

основание доказывает оператор (ч.3 ст.9), и доказательства собирают при запуске процесса

- дата согласия или факта, включившего основание
- субъект, а при представителе его полномочия
- пункт ч.1 ст.6 или норма ст.10, 11 и цель
- срок, статус и дата отзыва или отпадения

✕ **Основание на данные, а не на цель**
одно основание на всю клиентскую базу прячет рассылку, профилирование и передачи

✕ **Выбрали раз и навсегда**
договоры кончаются, согласия отзываются, а запись в реестре остается прежней

✕ **Обработка на отпавшем основании**
данные хранят после договора или отзыва и не уведомляют получателей

✕ **Основание после отзыва**
конструкция, впервые появившаяся в переписке об отзыве, выглядит злоупотреблением

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
DOP-007	Легальность	06 Допустимость
TRE-017	От монополии согласия к конкуренции оснований	01 Тренды
TRE-022	Отраслевые акты вместо согласий	01 Тренды
KAD-015	Гибридная модель распределяет основания по уровню риска	11 ПД работников

10.2

Согласие и обособление

- Обособление означает отдельный документ и отдельное действие
- Согласие работает за счет содержания, а не подписи
- Отзыв согласия прекращает только обработку на его основе
- Согласие за субъекта дает только тот, кому это разрешил закон

Обособление означает отдельный документ и отдельное действие

Ч.1 ст.9 152-ФЗ в редакции 156-ФЗ с 01.09.2025: два признака и шесть спорных зон

Privacy Advocates

Ч.1 СТ.9, С 01.09.2025

Два признака обособления

- визуальная и смысловая отдельность от договоров, ЛНА, анкет и иных сведений
- отдельное волевое действие, не слитое с подписанием договора или принятием соглашения
- требование касается любой формы, включая устную и конклюдентную
- суд указал: требования к надлежащему согласию на рекламу сложились практикой задолго до 01.09.2025 (анкета дисконтной карты, АС г. Москвы 20.04.2026, А40-311022/2025)

СПОРНАЯ ЗОНА	ОРИЕНТИР НА 2026 ГОД
отметка о согласии в типовой форме по пп."б" п.7 ПП-687	допустима в декларативной форме без подписи, вывод из письма Роскомнадзора от 03.10.2025
согласие на обороте анкеты или договора	допустимо, если подписывается как самостоятельный документ отдельным действием
типовой трудовой договор микропредприятия (ПП-858)	коллизия со ст.309.2 ТК не снята, надежнее приоритет ч.1 ст.9
модульное согласие, приложение к договору или ЛНА	регулятор не подтвердил и не исключил, нужна отдельная подпись по каждому блоку
общий текст с согласием на рекламу, изображение, тайну	спорно, надежнее раздельные волеизъявления
комплект документов под одной электронной подписью	спорно, отдельное действие на согласие надежнее

Практика: одна подпись под полисом и заявлением не оформляет сразу и договор, и согласие: предписание страховщику устояло в трех инстанциях, ВС отказал в передаче жалобы (А44-745/2017, 31.07.2018)

Согласие работает за счет содержания, а не подписи

Получатели, срок, цели и адресат согласия и информированность до волеизъявления

Схема свойств согласия
скачать

Privacy Advocates

получатели

Получатели поименно

обработчика называют с наименованием и адресом, категорий мало (А65-35933/2017)

срок

Срок конечный

по цели или сроку договора, а 10 лет после договора суд счел завышенными (А40-12838/2022)

цели

Цели по форме

одна цель на согласие нужна в письменной форме, в простом цели раскладывают по каждой

оператор

Один адресат

одно волеизъявление нескольким равноправным операторам Роскомнадзор устно не допускает

2%

ОПРОС СТРАХОВЩИКА, 2026

внимательно читают согласие

48% уверены, что без согласия сервисом не воспользоваться

ИНФОРМИРОВАННОСТЬ

- сведения доводят до волеизъявления, а не после отправки формы
- термины поясняют в тексте, отсылки к закону мало (А44-9647/2015)
- подпись и оговорка об отзыве дефект содержания не исцеляют (А65-35933/2017, А65-33540/2017)

Отзыв согласия прекращает только обработку на его основе

Отзыв согласия и требование о прекращении обработки: разные сроки, изъятия и последствия

Privacy Advocates

Отзыв согласия

ч.2 ст.9, ч.5 ст.21

привязан к согласию и действует только на будущее

- прекратить обработку и уничтожить данные в 30 дней, если они не нужны для целей и договор не говорит иного
- полный или частичный: по цели, каналу, оператору, получателю
- при ином основании, существовавшем независимо, обработку продолжают и мотивированно отвечают
- в письменном согласии способ отзыва указывают обязательно (п.8 ч.4 ст.9)

vs

Требование о прекращении

ч.5.1 ст.21

заявляется независимо от согласия

- исполнить в 10 рабочих дней, продление на 5 с мотивированным уведомлением
- не касается обработки по пп.2-11 ч.1 ст.6, ч.2 ст.10 и ч.2 ст.11
- квалифицируют по тексту обращения, при неясности уточняют
- путаница дает просрочку или отзыв без уничтожения данных

Особый порядок

маркетинг по ст.15: немедленно

распространение по ст.10.1: с момента требования

биометрия в ЕБС: оператору системы через Госуслуги

пациент: помощь не прекращается

Ошибки: отзыв обставляют формальностями тяжелее дачи согласия или уничтожают весь массив без разбора оснований, а основание, придуманное в момент отзыва, выглядит злоупотреблением правом

Согласие за субъекта дает только тот, кому это разрешил закон

Возрастные пороги, представители, наследники и пределы коллективных решений

Privacy Advocates

СУБЪЕКТ	КТО ДАЕТ СОГЛАСИЕ	ОПОРА И ОГОВОРКИ
младше 14 лет	законный представитель, достаточно подписи одного из родителей	письма Роскомнадзора от 29.12.2021 и 30.03.2023
от 14 до 18 лет	сам в пределах дееспособности по ст.26 ГК, вне их Роскомнадзор устно (14.08.2026) берет одно согласие представителя	спорно
пациент с 15 лет	сам по данным, связанным с медицинским вмешательством	ст.54 323-ФЗ, у отдельных категорий свои пороги
эмансипированный или в браке	сам, без возрастных ограничений	ст.21, 27 ГК, подтверждают решением или свидетельством
недееспособный	опекун, он же отзывает согласие	ч.6 ст.9 152-ФЗ, документ о назначении
умерший	наследники, если при жизни согласия не было (норму меняет проект № 1219127-8)	ч.7 ст.9 152-ФЗ, прижизненное согласие сохраняет силу
любой дееспособный	представитель по доверенности, нотариальная форма не нужна	кроме согласия на распространение (письмо Роскомнадзора от 02.12.2021)

Нельзя и можно: собрание собственников за участников согласие не дает, его решение ничтожно (кассация 88-5455/2024, новое рассмотрение). Подростку надежнее согласие за подписью его и представителя

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
BAZ-008	Когда нужна письменная форма согласия	03 Обзор комплаенса
KAD-004	Риск по согласию зависит от способа, формы и фиксации	11 ПД работников
TRE-007	Обособление согласия на обработку ПД с 01.09.2025	01 Тренды
KAD-005	Учет согласий ведут по каталогу атрибутов, а не одной отметкой	11 ПД работников
KAD-001	Согласие работника закон требует лишь в немногих случаях	11 ПД работников
POT-012	Согласие по умолчанию с графой "не согласен" уязвимо	12 ПД потребителей
MRK-002	Прямой маркетинг допустим только с предварительным согласием	13 Маркетинг
RSP-016	Согласие на распространение содержит девять реквизитов	14 Распространение
BIO-008	Биометрию дают только добровольно и отдельным согласием	15 Биометрия
SAJ-011	Клик по кнопке доказывают журналом действий пользователя	22 Сайт

10.3

Договор и закон

- Договорное основание покрывает данные только трех групп лиц
- Договорное основание кончается вместе с договором
- Основание п.2 ч.1 ст.6 требует нормы, которая предписывает обработку
- Публичные основания работают только в своих рамках

Договорное основание покрывает данные только трех групп лиц

Круг лиц п.5 ч.1 ст.6 152-ФЗ и тест необходимости по каждому потоку данных

Privacy Advocates

КТО В ДОГОВОРЕ	П.5
сторона договора, в том числе публичного и присоединения	покрыт
выгодоприобретатель или поручитель, включая застрахованного в коллективном страховании	покрыт
будущая сторона по своей инициативе: заявка, заказ, регистрация	покрыт
застрахованный без статуса выгодоприобретателя	нет
представитель, работник контрагента, родственник клиента	нет
работник, его кадровую обработку Роскомнадзор ведет по п.2	нет
односторонняя сделка вне договора: доверенность, зачет	нет

ТЕСТ НЕОБХОДИМОСТИ ПО ПОТОКУ

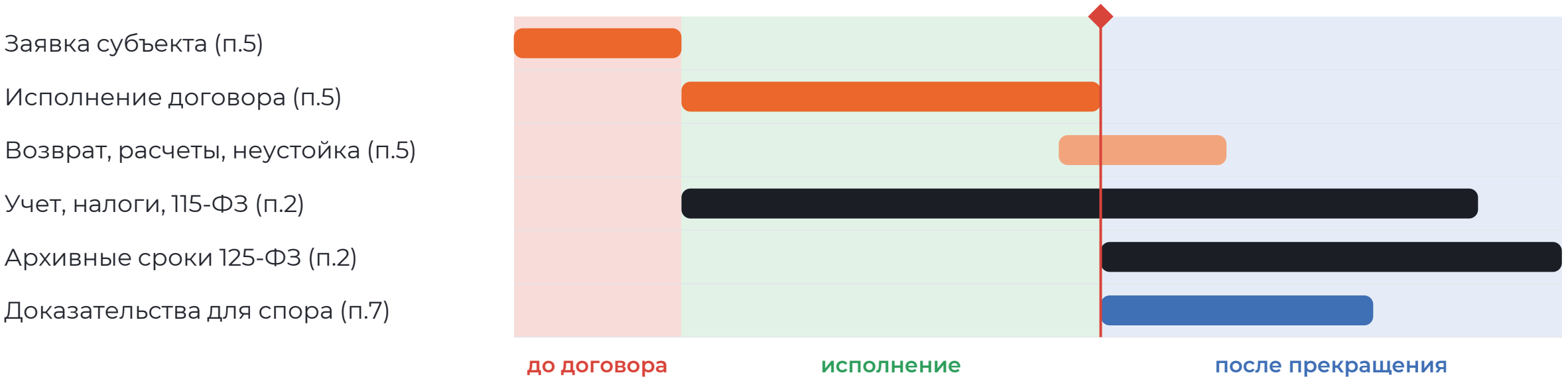
1. **Обязательства**
   выписать основные и отделить побочные условия
2. **Цель**
   по каждому обязательству без формулы "для исполнения договора"
3. **Связь**
   цель достигается именно этой обработкой и этим составом
4. **Альтернатива**
   нет менее интрузивного способа
5. **Остаток**
   отсеянное уходит на свое основание, продвижение только на согласие

Проверочный вопрос: перестанет ли оператор исполнять обязательство, если операцию не совершать. Доставка и онлайн-оплата входят в предмет, а профилирование для рекламы и запрос кредитного отчета (218-ФЗ) нет

Договорное основание кончается вместе с договором

Что держит обработку до заключения, при исполнении и после прекращения договора

Privacy Advocates



Инициатива
данные приходят в ответ на действие субъекта, а не из своей базы

Идентификация стороны
чужой договор основания не дает и при посреднике

Код из СМС
сам волю не доказывает: ВС требует проверить лицо

ОТПАДЕНИЕ ДОГОВОРА

- зафиксировать момент и причину
- обязательные сроки перевести на п.2
- остальное уничтожить за 30 дней
- архив отделить от активного

Основание п.2 ч.1 ст.6 требует нормы, которая предписывает обработку

П.2 ч.1 ст.6 152-ФЗ: две ветви, маркеры предписания и то, что основания не образует

Privacy Advocates

П.2 Ч.1 СТ.6 152-ФЗ

Две самостоятельные ветви

- цели международного договора РФ или закона
- функции, полномочия и обязанности по законодательству РФ, включая постановления Правительства, ведомственные и муниципальные акты
- оговорка "согласие не требуется" не условие основания

МАРКЕРЫ ПРЕДПИСАНИЯ В НОРМЕ

"оператор обязан" | "подлежат хранению" | "представляются" | "размещаются" | санкция за неисполнение

ОСНОВАНИЯ НЕ ОБРАЗУЮТ

- ✕ локальный акт оператора и иностранное право
- ✕ норма о субъективном праве, это путь к п.7 с оценкой
- ✕ общая отсылка к 152-ФЗ или к законодательству без статьи
- ✕ рекламные и закупочные нормы для маркетинга, там нужен п.1 и ст.15

Реестр: на каждую цель своя статья профильного акта. Слой держат ТК, НК и 402-ФЗ, социальное страхование и корпоративное право, а минимизация ограничивает исполнение: антитеррористическая защищенность не оправдывает копию паспорта посетителя

Публичные основания работают только в своих рамках

Суд, госуслуги, обязательное раскрытие, предписания органов и подрядчики в контуре обязанности

Privacy Advocates

ОСНОВАНИЕ	ЧТО ПОКРЫВАЕТ	ГРАНИЦА
п.3, судопроизводство	данные другой стороны в иске и процессуальных документах, передачу своему представителю	только в рамках процесса: ВС требует проверять, служили ли данные защите в деле (25-АД25-1-К4, направлено на новое рассмотрение), а сбор в обход суда не покрыт
п.4, госуслуги	обработку при оказании услуги по запросу заявителя	лишнее согласие не условие приема заявления (ВС, 5-КА19-56)
п.11, обязательное раскрытие	последующую обработку раскрытого: банкротство, закупки, педагоги	согласие на распространение не берут (А40-139096/2022, ВС отказал в передаче)
ст.15 закона о ФСБ, с 01.04.2026	передачу копии базы по предписанию, квалификация по п.2	проверяют форму, подпись и режим тайн, копии уничтожают по достижении целей
чч.4-6 ст.27 161-ФЗ, антифрод	обмен сведениями о переводах без согласия клиента	основание п.2, поэтому отзыв согласия обмен не останавливает

Подрядчик: привлеченное лицо основание не меняет, если закон не требует личного исполнения, объем данных минимален, а поручение оформлено по ч.3 ст.6 и с учетом ст.88 ТК. Аутсорсинг расчета зарплаты Пресненский районный суд признал правомерным (2-907/2024)

Договор с субъектом не вправе содержать три вида условий

Второе предложение п.5 ч.1 ст.6 152-ФЗ с 01.09.2022 и разъяснение Роскомнадзора от 03.07.2026

Privacy Advocates

ЗАПРЕЩЕННЫЕ УСЛОВИЯ ДОГОВОРА

Ограничение прав и свобод
положения, ограничивающие права и свободы субъекта ПД

ПД несовершеннолетних
положения, устанавливающие случаи их обработки, если иное не предусмотрено законодательством

Бездействие как условие
молчание и непроставленный отказ акцептом не считаются, запрет введен вместе с однозначностью согласия

КАК МЕНЯЛСЯ П.5

363-ФЗ от 21.12.2013 с 01.07.2014 добавил обработку при уступке прав, с 01.01.2017 уступку из пункта исключили, а 266-ФЗ с 01.09.2022 дополнил его **вторым предложением** с тремя запретами

РОСКОМНАДЗОР, 03.07.2026

Договор не допускает условий вопреки 152-ФЗ

- договор заключают по правилам гл.28 ГК, а обработка соблюдает принципы ст.5 152-ФЗ
- условие о передаче называет получателей и цели
- третьих лиц указывают поименно или ссылкой на ресурс оператора с их перечнем

Ревизия: оферты и договоры присоединения проверяют на три запрета и на сроки хранения, найденное недопустимое условие устраняют, а не смягчают формулировкой. Типовые пороки потребительских договоров разобраны в разделе 12

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
POT-002	С 01.09.2022 отказать в договоре за отказ дать ПД нельзя	12 ПД потребителей
POT-007	КС: договорное основание обеспечивает баланс сторон	12 ПД потребителей
TRE-019	Договор - средство, но не самоцель	01 Тренды
KAD-007	Закон и ТК легализуют кадровую обработку без согласия	11 ПД работников
KEJ-001	ПД работника передают без согласия по трудовому договору	32 Резонансные дела
FRM-004	Фармаконадзор идет по закону, без письменного согласия	35 Фармаконадзор

10.4

Законный интерес

- Законный интерес применим, только если выполнены три критерия
- Калькулятор находит неприменимость п.7 до оценки баланса
- Законный интерес не работает в зонах особого режима
- Оценку законного интереса оформляют протоколом

Законный интерес применим, только если выполнены три критерия

Конструкция п.7 ч.1 ст.6 152-ФЗ: две категории интереса и тест цели, необходимости и баланса

Privacy Advocates

1

Интерес и цель

актуальный интерес из реальной деятельности оператора, формализованный через конкретную цель

2

Необходимость

цель недостижима без этих данных и в этом объеме, менее интрузивной альтернативы нет

3

Баланс

права субъекта не нарушены: ожидания, информирование, уязвимость, законность источника

Категория 1

Субъективное право по норме

право участника и акционера на информацию (ст.65.2, 67 ГК), проверка полномочий представителя контрагента. Обоснование короткое: норма и невозможность реализовать право без обработки

или

Категория 2

Не запрещенная деятельность

антифрод, безопасность систем, бизнес-модель вытекают из диспозитивности и правоспособности. Нормы нет, и доказывание держится на описании деятельности, цели и необходимости

Важно: критерии не компенсируют друг друга, провал любого означает ч.1 ст.13.11 КоАП. Госорган собственного интереса не имеет, а КС жалобы на п.7 не принял (2173-О от 18.07.2019, 2029-О от 30.06.2026), но доказывать критерии по каждому процессу обязан оператор

Калькулятор находит неприменимость п.7 до оценки баланса

Три фильтра отрицательной селекции: допустимость, правомочность, пропорциональность

Калькулятор п.7 ч.1 ст.6 скачать

Privacy Advocates

МЕТОД: ТРИ ФИЛЬТРА

1. **Фильтр оснований**
   нет ли более подходящего или обязательного основания
2. **Фильтр норм**
   норма о праве или значимой цели, в строгом прочтении п.7 через союз "и"
3. **Фильтр обработки**
   нет ли особых режимов с потенциалом нарушения прав

РЕЗУЛЬТАТ ФИЛЬТРА

✓ пройден ! с замечаниями

✗ не пройден - неприменим

Селекция не заменяет оценку применимости, а отсекает ложные ожидания до нее

ПРИМЕР КАЛЬКУЛЯТОРА: ЧЕТЫРЕ ПРОЦЕССА

	Критерий фильтра	Пропуск	Подбор	Аудит	Инцидент
1.1	Обязательное по закону согласие	✓	✓	✓	✓
1.2	Случаи прямо из закона или договора	!	!	!	!
2.1	Нет прав оператора или третьих лиц	✓	✓	✓	✓
2.2	Нет норм об общественном интересе	!	-	-	-
3.1	Общедоступные источники, ст.8	✓	✓	✓	✓
3.2	Недееспособные и дети, ст.9	!	!	!	!
3.3	Специальные категории, ст.10	✓	!	!	!
3.4	Разрешенные для распространения, ст.10.1	✓	✓	✓	✓
3.5	Биометрия для идентификации, ст.11	✓	✓	✓	✓
3.6	Трансграничная передача, ст.12	✓	✓	✓	✓
3.7	Маркетинг и агитация через связь, ст.15	✓	✓	✓	✓
3.8	Автоматизированные решения, ст.16	✓	✓	✓	✓
3.9	Работники вне трудовых отношений, ТК	✓	-	!	!
3.10	Изображение и частная жизнь, ГК	✓	✓	✓	✓
3.11	Охраняемая тайна, ст.9 149-ФЗ	✓	✓	✓	✓
	Потенциальная применимость п.7	✓	✓	✓	✓

Процессы: пропускной режим, подбор соискателя с данными родственников, аудиты, расследование инцидентов. Замечания снимают минимизацией и гарантиями: договор с ИП или ФЛ (1.2), дети и спецкатегории (3.2, 3.3), аудиторы и консультанты ИБ (3.9)

Законный интерес не работает в зонах особого режима

Сценарии, где опора на п.7 выдерживает оценку, зоны неприменимости и типовые провалы

Схемы законного интереса
скачать

Privacy Advocates

Выдерживает оценку

- пропускной режим и безопасность объекта при идентифицирующем минимуме данных
- подготовка иска и передача данных суду, если сведения нельзя добрать в процессе
- проверка работника на конфликт интересов по открытым реестрам (ст.13.3 273-ФЗ)
- корпоративные права участника и акционера на документы общества
- хранение доказательств правомерности в пределах исковой давности

vs

Не работает

- прямой маркетинг, спецкатегории и судимость, биометрия, распространение, автоматизированные решения
- передача ПД работника третьим лицам, в том числе внутри группы (ст.88 ТК)
- банковская тайна, изображение и частная жизнь гражданина
- провалы оценки: продажа клиентской базы, обучение моделей на полной базе, пробив
- истребование чужих данных: интерес не обязывает другого их выдать

Поворот 2026: ресурсоснабжающие организации добивались от органов сведений регистрационного учета со ссылкой на законный интерес, но 28.05.2026 Верховный Суд эту линию скорректировал и в иске отказал (А72-10657/2024)

Оценку законного интереса оформляют протоколом

Процедура проверки применимости, поля протокола и связка с политикой и реестром обработки

Privacy Advocates

1. **Отсев**
   зоны неприменимости и специальные основания до теста
2. **Интерес и цель**
   право со ссылкой на норму или значимая цель
3. **Необходимость**
   минимум данных, менее интрузивной альтернативы нет
4. **Баланс и меры**
   ожидания, информирование, источники, гарантии
5. **Фиксация и пересмотр**
   протокол, реестр, политика, переоценка при смене цели

ПРОТОКОЛ ПО ПРОЦЕССУ

Восемь полей в четырех блоках

- процесс: субъекты, данные, операции, сроки
- дата, ответственный, участники
- допустимость, интерес с нормой, баланс
- решение, меры и итог: применимо, с мерами, неприменимо

ЛНА ОБ ОЦЕНКЕ

роли, порядок и сроки, критерии и признаки риска, шаблон протокола, типовые случаи

Высокий риск: несовершеннолетние, ТПД, распространение и свыше 100 тыс. субъектов оценку не останавливают, но требуют мер в решении. Методику выбирают одну и шаги разных методик не смешивают

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
TRE-020	Туманный законный интерес: понять - значит упростить	01 Тренды
KEJ-002	Проверка конфликта интересов по СПАРК - законный интерес	32 Резонансные дела
KEJ-003	Работодатель поручает обработку ПД работника без его согласия	32 Резонансные дела
KAD-011	Суд: обработку ПД работника нельзя ставить в зависимость от согласия	11 ПД работников

Основание выбирают под цель и доказывают заранее

Выводы раздела для DPO

Privacy Advocates

ГЛАВНОЕ

Основание привязано к паре цель и операция

не к массиву данных и не к оператору: сколько целей, столько записей об основании в реестре, и каждая доказывается документом, собранным при запуске процесса.

Законность проверяют в два шага: сначала основание по каждой цели, затем принципы ст.5, потому что основание необходимо, но недостаточно

Согласие проверяют последним

сначала закон, договор и законный интерес, согласие остается для целей без иного основания (письмо Роскомнадзора от 03.10.2025)

Согласие с 01.09.2025 обособлено

отдельный документ и отдельное действие, а пороки содержания не лечат ни подпись, ни оговорка об отзыве

Договор держит только необходимое

для стороны, выгодоприобретателя и поручителя и лишь пока действует договор, дальше хранение держат закон и интерес

Законный интерес оформляют протоколом

три критерия сразу, отсев зон неприменимости калькулятором и письменная оценка по каждому процессу

11

ПД работников

Как легализовать обработку ПД работников

11.1 Модель на согласии

11.2 Модель без согласия

11.3 Гибридная модель

Раздел на сайте
privacy-advocates.ru/pd/kad

11.1

Модель на согласии

- Согласие работника закон требует лишь в немногих случаях
- Согласие соискателя пишут под цели подбора и срок
- Модель на согласии проста, но дорога и хрупка
- Риск по согласию зависит от способа, формы и фиксации

Согласие работника закон требует лишь в немногих случаях

Нормы 152-ФЗ и ТК, по которым у работника берут письменное согласие

Privacy Advocates

НОРМА	КОГДА НУЖНО ПИСЬМЕННОЕ СОГЛАСИЕ РАБОТНИКА
ст.8 152-ФЗ	включение ПД в общедоступные источники, например в корпоративный справочник
ст.10 152-ФЗ	обработка специальных категорий ПД, кроме сведений о здоровье, относящихся к возможности выполнять трудовую функцию
ст.10.1 152-ФЗ	обработка ПД, разрешенных работником для распространения, по отдельной форме
ст.11 152-ФЗ	обработка биометрических ПД, например проход по биометрии наряду с альтернативным способом
ст.16 152-ФЗ	принятие решений на основании исключительно автоматизированной обработки ПД
п.3 ст.86 ТК	получение ПД не от самого работника, с предварительным уведомлением о нем
абз.2 ст.88 ТК	сообщение ПД работника третьей стороне, кроме случаев, установленных федеральным законом
абз.3 ст.88 ТК	сообщение ПД работника в коммерческих целях

На практике еще: добровольные блага вроде ДМС, кадровый резерв и внешние HR-платформы. Ориентиры - разъяснения Роскомнадзора от 14.12.2012, письмо Минцифры от 28.08.2020 № ЛБ-С-074-24059 и типовой трудовой договор микропредприятия (ПП от 27.08.2016 № 858)

Согласие соискателя пишут под цели подбора и срок

Образец согласия на подбор персонала и что учесть в нем в 2026 году

Privacy Advocates

1 **Цели**

поиск и оценка соискателей, проверка благонадежности, решение о приеме

2 **Состав ПД**

около 30 позиций: от ФИО и контактов до трудовой деятельности и воинского учета

3 **Способы**

смешанная обработка, передача по внутренней сети и через интернет

4 **Источники**

сам соискатель, открытые источники, контрагенты и имеющиеся данные

5 **Получатели**

обработчики, компании группы и контрагенты, включая ТПД

ЧТО УЧЕСТЬ В 2026 ГОДУ

- с 01.09.2025 согласие оформляют отдельно от анкеты и иных документов (ч.1 ст.9 152-ФЗ)
- Роскомнадзор устно (14.08.2026) требует согласия при отборе, но не при немедленном приеме и на рекрутинговых платформах
- парсинг соцсетей для подбора рискован, а отказ рассматривать кандидата без согласия задевает ст.64 ТК

СРОК ДЛЯ НЕПРИНЯТОГО КАНДИДАТА

Три ориентира

- **30 дней** по письму Минцифры
- **до 6 месяцев** по устной позиции Роскомнадзора (31.01.2024)
- **3 месяца**, пока кандидат может оспорить отказ в найме (ст.391, ч.1 ст.392 ТК)
- кадровый резерв ведут по отдельному согласию

Модель на согласии проста, но дорога и хрупка

Аргументы за и против общепрактикуемой легализации обработки ПД работников на согласии

Privacy Advocates

ЗА

Почему модель популярна

- простой концепт, прямо предусмотренный нормами ТК
- соответствует ожиданиям надзорных органов
- получить ПД не от работника можно только с его согласия (п.3 ст.86 ТК)
- Роскомнадзор допускает согласие в электронной форме

ПРОТИВ

- ✕ большие затраты времени и денег на сбор согласий, затем бремя их администрирования и хранения
- ✕ не все работники готовы подписать обновленное согласие, а подписанное отзывается в любой момент
- ✕ работник вправе собственноручно править текст типового согласия
- ✕ иллюзия, что отзывом можно запретить обработку, хотя трудовая обработка идет на основании ТК и договора
- ✕ по позиции Роскомнадзора согласие прекращается с увольнением, и для передачи архива бывшего работника нужно новое
- ✕ письменное согласие подчиняется ч.4 ст.9 (одна цель - одно согласие), а с 01.09.2025 оформляется отдельно от иных документов
- ✕ истребование согласия суд может счесть дискриминацией (88-17959/2020, направлено на новое рассмотрение)

Риск по согласию зависит от способа, формы и фиксации

Чем пассивнее способ и слабее доказуемость формы, тем выше риск санкций

Схема модели согласия
скачать

Privacy Advocates

СПОСОБ ВЫРАЖЕНИЯ И ВЕРОЯТНОСТЬ САНКЦИЙ

Double opt-in
отметка и подтверждение по ссылке из письма — низкая

Single opt-in
субъект сам ставит отметку в пустом поле — низкая

Silent opt-in
предустановленная отметка или кнопка с оговоркой — средняя

Silent opt-out
предустановлено несогласие, субъект его не снимает — средняя

Soft opt-out
отметка о несогласии или двойное отрицание — высокая

Hard opt-out
новые условия приняты без письменного отказа в срок — высокая

ФОРМА ПОЛУЧЕНИЯ И РИСК ПО ДОКАЗУЕМОСТИ, ЭКСПЕРТНЫЙ ПОДХОД

ФОРМА	РИСК	КОГДА ГОДИТСЯ И ЧТО СНИЖАЕТ РИСК
Письменная	низкий	обязательна только в случаях из закона, главный риск в неполных реквизитах ч.4 ст.9
Электронная, КЭП	низкий	равнозначна бумаге в силу закона, соглашения не нужны (ч.4 ст.9 152-ФЗ, ст.6 63-ФЗ об ЭП)
Электронная, ПЭП или НЭП	средний	равна бумаге по закону или при соглашении об электронном взаимодействии, иначе код из СМС дает обычное согласие
Конклюдентная	средний	отметка, регистрация, оплата. Доказывает журнал событий, письменную форму не заменяет
Устная	высокий	трудно доказуема: нужны идентификация, зачитанные условия и запись разговора

МЕТОД ФИКСАЦИИ

с 01.09.2025 согласие оформляют отдельно от другой информации и документов (ч.1 ст.9). По экспертному подходу и по телефону вопрос о согласии задают отдельно

Учет согласий ведут по каталогу атрибутов, а не одной отметкой

Общий каталог атрибутов согласия для группы компаний с общей клиентской базой

Privacy Advocates

Стороны

- идентификатор клиента у каждого участника без единой записи группы
- операторы ПД
- обработчики ПД
- получатель согласия, включая партнеров

Факт согласия

- дата и время получения
- способ выражения: opt-in, opt-out и др.
- канал: сайт, приложение, бумага, колл-центр

Предмет

- цели с учетом продуктов каждого участника
- действия с ПД
- состав ПД
- срок обработки
- разрешение на рекламу по каналам: телефон, SMS, e-mail, push

Изменения и отзыв

- дата, время и содержание полного или частичного отзыва
- актуальный перечень операторов и партнеров
- дата и содержание возражения против изменения перечня
- актуализация ПД субъектом
- информирование об удалении ПД

Практика 2026: Роскомнадзор устно (14.08.2026) не допускает одно согласие нескольким равноправным операторам, поэтому у каждой компании группы свое согласие, а при конфликте статусов в системах побеждает отказ

Работнику объясняют, зачем компании его согласие

Четыре ответа для коммуникации с персоналом при сборе согласий

Privacy Advocates

Зачем компании мое согласие?

чтобы вести бизнес, удерживать позиции на рынке и выполнять обязательства перед вами, клиентами и партнерами

Как защищены мои данные у партнеров?

передача клиентам и партнерам идет по вашему письменному согласию, а получатели связаны с компанией соглашением о конфиденциальности

Что будет без согласия?

компания не сможет передать данные провайдерам и подрядчикам, а значит обеспечить вас бенефитами

Что я узнаю из согласия?

цель, объем и содержание обработки ваших ПД и срок действия согласия

ГДЕ СОГЛАСИЕ ДЕЙСТВИТЕЛЬНО НУЖНО

Узкие зоны

- передача ПД работника третьим лицам, кроме случаев из закона (ст.88 ТК)
- подрядчики и облачные сервисы - поручение по ч.3 ст.6 152-ФЗ и письменное согласие каждого работника (Управление Роскомнадзора по Курской области, 18.06.2026)
- добровольные блага и кадровый резерв

Честная граница: обычная кадровая работа идет на основании закона и отзывом согласия не останавливается, и так это и объясняют работнику

11.2

Модель без согласия

- Закон и ТК легализуют кадровую обработку без согласия
- Регуляторы допускают передачу ПД работника без согласия
- Суды признают договорное основание в трудовых отношениях
- Льготы работника нельзя ставить в зависимость от согласия

Закон и ТК легализуют кадровую обработку без согласия

Основания ч.1 ст.6 152-ФЗ и нормы ТК о договоре, распорядке и локальных актах

Privacy Advocates

Ч.1 СТ.6 152-ФЗ

п.2. Обязанности оператора
осуществление и выполнение функций, полномочий и обязанностей, возложенных на оператора законом

п.5. Договор
исполнение договора, стороной которого является субъект ПД

п.7. Законный интерес
осуществление прав и законных интересов оператора или третьих лиц, если не нарушаются права и свободы субъекта

СТАТЬЯ ТК	ЧТО ДАЕТ РАБОТОДАТЕЛЮ
ст.8	принимать локальные нормативные акты в пределах компетенции
ст.15	трудовые отношения - соглашение о личном выполнении функции под управлением и контролем работодателя
ст.21	работник обязан исполнять трудовой договор и соблюдать правила распорядка
ст.22	требовать исполнения трудовых обязанностей и соблюдения распорядка
ст.57	включать в договор условия, не ухудшающие положение работника, в том числе о неразглашении тайны

Сейчас: цели кадровой обработки закрыты перечнем п.1 ст.86 ТК, а Роскомнадзор устно (28.01.2022) рассматривает ее через п.2 ч.1 ст.6, а не через договор. Поэтому базовым основанием фиксируют обязанности по трудовому законодательству

Регуляторы допускают передачу ПД работника без согласия

Позиции Минцифры 2020 года и Роскомнадзора 2012 года о кадровой обработке

Privacy Advocates

Минцифры, 28.08.2020

Письмо № ЛБ-С-074-24059

методические рекомендации для общеобразовательных организаций

- согласие не требуется при передаче ПД работника в связи с должностными обязанностями, в том числе при командировании по правилам гостиничных услуг (в письме ПП № 490, сейчас ПП от 27.11.2025 № 1912)
- положения законодательства о ПД включают в трудовые договоры, должностные регламенты и иные локальные акты
- по смыслу письма это мера ознакомления работников, которые сами обрабатывают ПД (п.6 ч.1 ст.18.1), а не легализация обработки их данных

vs

Роскомнадзор, 14.12.2012

Разъяснения о работниках, соискателях и резерве

- обработка без согласия в случаях из коллективного договора, правил распорядка, соглашений и локальных актов, принятых по ст.372 ТК
- согласие не нужно при передаче ПД работника или служащего в связи с должностными обязанностями, включая командировку
- пропускной режим без согласия, если работодатель ведет его сам или по коллективному договору и локальным актам

В 2026 году: Роскомнадзор устно (14.08.2026) не требует согласия для зарплатного проекта при заявлении работника, но Роструд 07.10.2026 считает выпуск карты без заявления незаконным, а для подрядчиков нужны поручение и письменное согласие

Суды признают договорное основание в трудовых отношениях

Практика об обработке ПД работников, часть 1 из 3

Privacy Advocates

ВС РФ, 01.07.2019, № 67-КГ19-5

Трудовые отношения длятся дольше договора

ТК регулирует и отношения, производные от трудовых (ст.5): они возникают до договора, сопровождают его и сменяют после увольнения. Вывод о прекращении всех прав и обязанностей сторон с расторжением договора неправомерен

ВС Удмуртии, 25.01.2012, № 33-198/2012

работодатель обрабатывал ПД своего работника, отношения основаны на трудовом договоре, и согласие в силу п.5 ч.1 ст.6 152-ФЗ не обязательно

9 ААС, 09.02.2022, № 09АП-87227/2021

п.5 ч.1 ст.6 - общая норма без исключения для трудовых отношений: передача ПД работников для ДМС, санаторно-курортного лечения и размещения исполняет коллективный договор

АС Московского округа, 30.05.2022

позиция по делу Аэрофлота подтверждена, кассационная жалоба Роскомнадзора отклонена

Льготы работника нельзя ставить в зависимость от согласия

Практика об обработке ПД работников, часть 2 из 3

Privacy Advocates

Прав не нарушил

СПб горсуд, 24.01.2012, № 33-712/2012

фамилия работника в конструкторской документации указана при исполнении трудовых обязанностей по должностной инструкции и ст.86 ТК

vs

Нарушение

3 КСОЮ, 01.02.2021, № 88-714/2021

в ДМС и компенсации питания отказали без согласия на передачу ПД разным организациям, а нужность такой передачи для льгот работодатель не доказал

- компенсация 25 000 ₽ оставлена в силе
- тот же суд 16.12.2020 (№ 88-17959/2020) указал на признаки дискриминации и направил дело на новое рассмотрение

ВСТРЕЧНАЯ ЛИНИЯ

СПб горсуд, 07.09.2023, № 33-16277/2023

форму согласия для добровольной льготы определяет работодатель и его договор со страховщиком, и отказ в льготе без такого согласия правомерен

БЕЗОПАСНАЯ ЛИНИЯ

- под каждую цель свой документ согласия
- объем данных ограничен целью блага
- отказ от блага не влечет последствий для трудовых прав

Суд: обработку ПД работника нельзя ставить в зависимость от согласия

Практика об обработке ПД работников, часть 3 из 3

Privacy Advocates

Обработка ПД в трудовых отношениях ведется в рамках исполнения трудового договора и закона и **не может ставиться под условие** получения согласия, иное приводило бы к невозможности заключения и исполнения договора

Решение Пресненского районного суда г. Москвы от 30.01.2024 № 2-907/2024

ПРЕСНЕНСКИЙ СУД, 2024

работодатель вправе передавать ПД и поручать их обработку третьим лицам в собственном законном интересе, если права работников не нарушены

КЕМЕРОВО, 30.09.2022

1. проверка по открытому источнику, не занимает ли работник иную должность, по локальному акту о конфликте интересов (ст.11, 13.3 273-ФЗ) опирается на п.7 ч.1 ст.6 152-ФЗ
2. отказ в возбуждении дела по ч.2 ст.13.11 КоАП устоял (№ 12-532/2022)

Наблюдение за работником ограничено четырьмя условиями

Видеонаблюдение, служебные устройства и алкотестер: позиции Роструда, Роскомнадзора и судов

Privacy Advocates

1. **Цели**
   закрытый перечень п.1 ст.86 ТК, иную цель наблюдением не обосновать
2. **Время и место**
   за пределами рабочего времени и места нужно отдельное обоснование, которого обычно нет
3. **Зона приватности**
   места, где работник вправе рассчитывать на приватность даже в рабочее время
4. **Соразмерность**
   непрерывная фиксация не проходит там, где достаточно периодической проверки

ИНСТРУМЕНТ	ПОЗИЦИЯ	ОПОРА
Видеонаблюдение	Роструд требует ЛНА под роспись и письменное согласие, Роскомнадзор устно видит основание п.2 ч.1 ст.6	спорно
Скрытая камера	скрытность оценивают по осведомленности: ЛНА, допсоглашение, табличка	2-2969/2019
Служебные устройства	контролируют оборудование и учетные записи, на личное устройство только с согласия	п.8 ст.86 ТК
Алкотестер	только с согласия работника, отказ от теста не прогул	Роструд, 2021 и 2023

Порядок: наблюдение вводят локальным актом под роспись и условием трудового договора, а действующих работников уведомляют, при изменении условий труда за два месяца (ч.2 ст.74 ТК)

11.3

Гибридная модель

- Модель договора и локальных актов оптимальна, но рискованна
- Раздел о ПД в трудовом договоре защищает обе стороны
- Гибридная модель распределяет основания по уровню риска

Модель договора и локальных актов оптимальна, но рискованна

Аргументы за и против перспективной модели легализации обработки ПД работников

Privacy Advocates

ЗА

- трудовые отношения и так регулируются договором и внутренним распорядком
- ТК и федеральные законы допускают передачу ПД работника не только по согласию
- Минцифры (28.08.2020) и Роскомнадзор (14.12.2012) не требуют согласия при передаче ПД в связи с должностными обязанностями
- суды признали п.5 ч.1 ст.6 основанием передачи ПД работников (дело А40-163911/2021)

ПРОТИВ

- Роскомнадзор относит п.5 ч.1 ст.6 к гражданско-правовым договорам, а кадровую обработку - к п.2 ч.1 ст.6 и гл.14 ТК (28.01.2022)
- согласия письменной формы в трудовой договор не включают (31.01.2024), а ТПД и передачу третьим лицам ведут по письменному согласию по ст.88 ТК (15.05.2024)
- условия договора об обработке ПД могут счесть ухудшающими положение работника (ст.9, 57 и п.9 ст.86 ТК)

ЦЕНА ОШИБКИ

Возможные последствия

- организации - штраф до 700 тыс. ₽, повторно до 1,5 млн ₽ (ч.2 и 2.1 ст.13.11 КоАП)
- должностным лицам - до 300 тыс. ₽, повторно до 500 тыс. ₽
- иски субъектов, обычно до 30 тыс. ₽ на истца
- переделка процессов по предписанию, обычно за 6 месяцев
- негативный образ в СМИ и ущерб деловой репутации организации и ее менеджеров

Раздел о ПД в трудовом договоре защищает обе стороны

Что работник подписывает в трудовом договоре и зачем Компании этот раздел

Privacy Advocates

1. **Основание**
   обработка для заключения, исполнения, изменения и прекращения договора и для исполнения законов и локальных актов идет по договору и закону (пп.2 и 5 ч.1 ст.6), согласие для этого не нужно
2. **Где правила**
   цели, состав, действия, сроки и защиту ПД определяют закон, договор и локальные акты, а при необходимости согласие работника
3. **Обязанности Компании**
   обрабатывать только нужные ПД, защищать их и создавать работнику условия для работы с ПД других людей
4. **Права работника**
   доступ к своим ПД, их уточнение, блокирование и уничтожение, если они неполные, неточные или не нужны
5. **Обязанности работника**
   обрабатывать ПД других людей только в целях и порядке, которые установлены правилами Компании, и беречь их

ЗАЧЕМ

Три выгоды для работника

- период обработки ваших ПД ограничен
- Компания обязана создать условия для обработки и защиты ПД
- ваши права на ПД закреплены в договоре

СРОК В ШАБЛОНЕ

5 лет после увольнения

условие образца договора: столько Компания вправе обрабатывать ПД после прекращения отношений, если иной срок не установлен соглашением или законом

Гибридная модель распределяет основания по уровню риска

Трудовой договор, локальные акты и точечные согласия в трудовых и связанных с ними отношениях

Privacy Advocates

ЗОНА ОБРАБОТКИ	ОПОРА	РИСК	КАК СНИЗИТЬ РИСК
заключение, исполнение, изменение и прекращение договора, права и обязанности по закону и ЛА, обработка до окончания связанных обязательств	ТД и ЛА	низкий	описать в ЛА цели, состав и источники ПД, действия и сроки хранения
непрерывная работа и должностные обязанности: доверенности, электронная подпись, служебная связь	ЛА	низкий	закрепить в ЛА и ознакомить работника под подпись
корпоративные блага: ДМС, мотивационные и образовательные программы	ЛА и заявление	средний	opt-in по заявлению работника и opt-out с прекращением обработки
ТПД, передача третьим лицам и в коммерческих целях, получение не от работника, общедоступные источники, передача архиву после увольнения, автоматизированные решения	ЛА и согласие	высокий	отдельное письменное согласие по ч.4 ст.9, обособленное с 01.09.2025, и норма ЛА об осведомленности работника
специальные категории, кроме сведений о здоровье для трудовой функции, ПД для распространения, биометрия, судимость	закон	высокий	только в случаях и порядке, прямо предусмотренных законом

Эффект: при отзыве согласия на чувствительную операцию прекращается только она, а обязательная обработка сохраняет опору на закон и локальные акты

12

ПД потребителей

Договор с потребителем, запрет избыточного сбора и ПД детей

12.1 Договор и ст.16 ЗоЗПП

12.2 Позиции КС, ЦБ, РКН, ФАС и практика

12.3 ПД детей

Раздел на сайте
privacy-advocates.ru/pd/pot

12.1

Договор и ст.16 ЗоЗПП

- Договор с субъектом не может ограничивать его права
- С 01.09.2022 отказать в договоре за отказ дать ПД нельзя
- Ущемляющие условия договора ничтожны, в том числе о ПД
- Потребитель вправе узнать, зачем у него просят ПД

Договор с субъектом не может ограничивать его права

Редакция п.5 ч.1 ст.6 152-ФЗ с 01.09.2022 и типовые пороки потребительских договоров

Privacy Advocates

Заключаемый с субъектом ПД договор не может содержать положения, **ограничивающие права и свободы** субъекта, устанавливающие случаи обработки ПД несовершеннолетних, если иное не предусмотрено законодательством, а также положения, допускающие в качестве условия заключения договора **бездействие субъекта**

п.5 ч.1 ст.6 152-ФЗ в редакции 266-ФЗ от 14.07.2022

ПОРОКИ ПО РОСКОМНАДЗОРУ

1. бездействие субъекта как подтверждение акцепта оферты
2. передача ПД неопределенному кругу лиц, в том числе для рекламы
3. обработка в целях, не связанных с предметом договора
4. бессрочная обработка ПД

Последствие: обработка на таких условиях договора - это обработка без основания по ч.1 ст.13.11 КоАП, с 30.05.2025 для организаций штраф 150-300 тыс. ₽, а пороки Роскомнадзор назвал на дне открытых дверей 29.09.2022

С 01.09.2022 отказать в договоре за отказ дать ПД нельзя

135-ФЗ от 01.05.2022 дополнил ст.16 ЗоЗПП прямым запретом обусловливания

Privacy Advocates

Продавец, исполнитель или владелец агрегатора **не вправе отказывать** потребителю в заключении, исполнении, изменении или расторжении возмездного договора из-за отказа предоставить ПД. Исключения два: обязанность предоставить данные установлена законодательством либо **непосредственно связана с исполнением договора** (п.4 ст.16 ЗоЗПП)

Потребитель

гражданин, который намерен заказать или приобрести либо заказывает, приобретает или использует товары, работы и услуги для личных нужд, не связанных с предпринимательством

Продавец

организация любой формы или ИП, реализующие товары потребителям по договору купли-продажи

Исполнитель

организация любой формы или ИП, выполняющие работы или оказывающие услуги потребителям по возмездному договору

Владелец агрегатора

владелец программы или сайта, где потребитель знакомится с предложением продавца, заключает договор и вносит предоплату

Следствие: статус потребителя возникает уже на стадии намерения, поэтому запрет действует и для калькуляторов, заявок и консультаций до договора, а маркетплейс отвечает за поля своей формы наравне с продавцом

Ущемляющие условия договора ничтожны, в том числе о ПД

Недопустимые условия по п.2 ст.16 ЗоЗПП и рекомендации для потребительских договоров

Privacy Advocates

НЕДОПУСТИМЫЕ УСЛОВИЯ, П.2 СТ.16 ЗОЗПП

Подп.1. Одностороннее изменение

право продавца, исполнителя или агрегатора на односторонний отказ от обязательства или изменение предмета, цены, срока и иных условий, если закон такого права не допускает

Подп.5. Навязывание

обусловливание приобретения одних товаров или услуг обязательным приобретением других, в том числе заключением иных договоров

Подп.15. Иные нарушения

условия, нарушающие правила международных договоров, ЗоЗПП и иных актов о защите прав потребителей

РЕКОМЕНДАЦИИ

Как писать договор

- выделить специальный раздел с исчерпывающим описанием условий обработки ПД
- не закладывать резиновые формулировки для одностороннего изменения состава операторов и обработчиков
- не навязывать обработку ПД компаниями группы и участниками экосистемы
- не включать в договор согласие на обработку в целях, отличных от его исполнения

В 2026 году: недопустимые условия ничтожны (п.1 ст.16), их включение наказывается по ч.2 ст.14.8 КоАП, потребители отсуживают ничтожность навязанных согласий, а с 01.09.2025 согласие и вовсе оформляется отдельно от договора

Потребитель вправе узнать, зачем у него просят ПД

Процедура п.4 ст.16 ЗоЗПП: срок, форма ответа и что подготовить заранее

Privacy Advocates

1

Запрет

нельзя отказать в договоре за отказ дать ПД, если их сбор не обязателен по закону и не связан с исполнением договора

2

Требование

потребитель вправе запросить конкретные причины и правовые основания, по которым договор без ПД невозможен

3

Письменно

в том числе электронным документом - ответ в течение 7 дней со дня требования

4

Устно

информация предоставляется незамедлительно

5

Форма ответа

та же, в которой предъявлено требование, если в нем не указано иное

- проанализировать состав ПД потребителя на минимизацию и обосновать каждое поле нормой или предметом договора
- закрепить в локальных актах процедуру ответа и альтернативу покупки без предоставления ПД
- учесть все формы, в которых может прийти требование потребителя
- подготовить инструкцию и провести тренинг для персонала, работающего с потребителями

Тест поля: назовите норму, которая обязывает собирать поле, или действие по договору, невыполнимое без него. Если нельзя назвать ни то, ни другое, поле избыточно, а общая ссылка на политику обработки обязанность не исполняет

Обусловливание услуги ПД наказывается по ст.14.8 КоАП

Ч.7 и 8 ст.14.8 КоАП и надзорная практика по потребительским данным 2023-2026 годов

Privacy Advocates

5-10 тыс. ₽

Должностные лица

ч.7 ст.14.8 за отказ в договоре из-за отказа дать ПД, с 01.09.2022 по 145-ФЗ

30-50 тыс. ₽

Юридические лица

ч.7 ст.14.8, если ПД не обязательны по закону и не нужны для исполнения договора

200-500 тыс. ₽

Отказ за отказ от биометрии

ч.8 ст.14.8 для организаций с 30.05.2025, для должностных лиц 50-100 тыс. ₽

СЮЖЕТ	ПОЗИЦИЯ	ИСТОЧНИК
Копия паспорта у оператора связи	избыточна в части сведений, не нужных для договора, в том числе при расторжении через чат	Роспотребнадзор, вебинар 27.07.2023
Паспорт для возврата денег на карту	избыточен, платежный инструмент уже идентифицирует получателя, штраф устоял в первой инстанции	А75-29509/2025, 12.03.2026
Биометрия для выдачи банковской карты	обусловливание запрещено, банку объявлено предостережение	Роспотребнадзор, 19.01.2024
СНИЛС для платных медуслуг	предоставляется по усмотрению гражданина	письмо Минздрава 18.01.2024 № 31-2/63 по ПП № 736, теперь ПП № 659

С 01.10.2026 у платформ появился второй слой требований

289-ФЗ о платформенной экономике: обязанности владельца и оператора посреднической платформы по данным

Privacy Advocates

289-ФЗ ОТ 31.07.2025

В силе с 01.10.2026

закон вводит понятия цифровой и посреднической платформы, владельца, оператора, партнера, пункта выдачи и карточки товара. Посреднической платформа становится с включения в реестр

Защита сведений

владелец любой платформы защищает сведения на ней по законам об информации и о ПД

Проверка партнера

оператор посреднической платформы проверяет партнера по ЕГРЮЛ, ЕГРИП или через ЕСИА

Алгоритмы

оператор вправе подбирать исполнителя и считать вознаграждение алгоритмом, а ограничивать заказы только им, исполнитель-гражданин вправе знать об этом

Ограниченные товары

продажа при идентификации покупателя через ЕБС по ст.10 572-ФЗ или иным способом, который установит Правительство

Зарубежный контур: к иностранному оператору платформы из реестра могут применяться меры понуждения по ст.9 236-ФЗ, как к иностранным интернет-компаниям

12.2

Позиции КС, ЦБ, РКН, ФАС и практика

- КС: договорное основание обеспечивает баланс сторон
- Маркетинг и биометрия заемщика требуют отдельных согласий
- Согласие на биометрию вводом кода суды признали ничтожным
- Даже госсервис просит согласие, которое нельзя отозвать

КС: договорное основание обеспечивает баланс сторон

Определение Конституционного Суда от 17.07.2018 № 1810-О о п.5 ч.1 ст.6 152-ФЗ

Privacy Advocates

П.5 ч.1 ст.6 152-ФЗ направлен на реализацию принципа **надлежащего исполнения обязательств** (ст.309 ГК), обеспечивает защиту прав участников договорных отношений, в том числе по коммунальным услугам, и справедливый баланс их законных интересов

Определение КС РФ от 17.07.2018 № 1810-О

ЖАЛОБА

ресурсоснабжающая организация использовала личный номер телефона заявительницы без ее согласия

ДОВОД

норма нарушает баланс сторон договора о коммунальных услугах и отдает приоритет интересам юридического лица (ст.17, 24 и 46 Конституции)

ИТОГ

КС отказал в принятии жалобы к рассмотрению

Граница: договор покрывает только обработку, необходимую для его исполнения. По устной позиции Роскомнадзора (14.08.2026) это большинство отношений, но продвижение и иные цели требуют своего основания

Маркетинг и биометрия заемщика требуют отдельных согласий

Информационное письмо Банка России и Роскомнадзора от 29.07.2021 № ИН-06-59/57, 08ЛА-48666

Privacy Advocates

Без согласия

Заключение и исполнение договора

п.5 ч.1 ст.6 152-ФЗ позволяет обрабатывать ПД заемщика без согласия для заключения договора по его инициативе и исполнения договора потребительского кредита (займа)

Только с согласием

Иные цели и третьи лица

обработка в других целях, поручение обработки другому лицу и раскрытие ПД третьим лицам возможны только с согласия заемщика (ч.2 ст.5, ч.3 ст.6, ст.7)

Отдельные согласия

Маркетинг и биометрия

для продвижения товаров и услуг и для биометрических ПД кредиторам рекомендовано брать отдельные согласия с учетом ч.1 ст.9, ст.11 и ст.15

С 2025 года: с 01.09.2025 любое согласие оформляется отдельно от иных документов (ч.1 ст.9 в редакции 156-ФЗ), так что рекомендация 2021 года стала общим правилом, а по каждому получателю нужна отдельная отметка

Согласие на биометрию вводом кода суды признали ничтожным

История клиента банка 2023 года и позиция судов 2025 года

Privacy Advocates

1

28.09.2023: возражение

клиент пишет в чат банка возражение против размещения его биометрии в ЕБС и требует уничтожить ее до 30.09.2023

2

05.11.2023: банкомат

клиент снимает деньги. При вводе PIN-кода на экране строка "Продолжая, вы соглашаетесь...", а отказаться можно кнопками "Отказаться" и "Понятно"

3

Ответ поддержки

вы дали согласие на биометрию, скорее всего в банкомате: именно в этот день вы снимали там деньги

4

2025: суды

согласие на биометрию, данное вводом одноразового кода при входе в личный кабинет, признано ничтожным

ЧТО ДЕЛАТЬ КЛИЕНТУ

- читать текст на экране до ввода PIN-кода
- нажать "Отказаться", если не согласны
- проверить биометрию на Госуслугах
- отозвать лишние согласия

Итог: Вологодский областной суд 18.03.2025 (33-802/2025), Третий КСОЮ оставил решение в силе 04.08.2025 (88-14185/2025). Читайте, что написано на экране, прежде чем вводить PIN-код

Даже госсервис просит согласие, которое нельзя отозвать

Текст согласия в личном кабинете налогоплательщика при оплате налогов через банк

Privacy Advocates

Предоставляю Федеральной налоговой службе осуществлять **все действия (операции)** с моими персональными данными... и передачу в кредитную организацию... В случае отзыва согласия... Федеральная налоговая служба **вправе не прекращать их обработку** до окончания срока действия настоящего согласия

"Соглашение об обработке персональных данных" в личном кабинете налогоплательщика

ЧТО НЕ ТАК

1. документ назван соглашением, хотя это согласие
2. "все действия" вместо конкретного перечня
3. отзыв ничего не меняет, а значит, выбора у человека нет
4. если обработка идет по закону, согласие только создает видимость выбора

По закону: после отзыва согласия обработку прекращают, если нет иного основания (ч.2 ст.9), а ПД уничтожают в 30 дней (ч.5 ст.21). Пишите согласия так, чтобы отзыв что-то значил

Согласие на рекламу без права отказаться недобросовестно

Информационное письмо Банка России и ФАС от 06.09.2021 № ИН-06-59/70, АК/75514/21

Privacy Advocates

Недобросовестно

Согласие без выбора

кредиторы: банки, МФО, кредитные кооперативы, ломбарды

согласие на получение рекламы включено в договор займа, заявление или иной документ, а заемщик не может отказаться от него при заключении договора, хотя законы о рекламе и о связи требуют предварительного согласия абонента

- Роскомнадзор (29.09.2022) тоже против маркетинговых согласий в тексте договора и не рекомендует встраивать их в договор

vs

Рекомендуется

Отдельная подпись или отметка

в том числе в электронных документах дистанционных каналов

- обеспечить заемщику отдельную подпись или отметку о согласии на рекламу
- указать перечень конкретных рекламораспространителей - кредитора и третьих лиц
- лучшая практика - отдельный документ, отказ от которого не влияет на договор

Практика: ВС 22.06.2026 допустил согласие на рекламу в обмен на скидку, если покупка без него доступна (А07-5689/2025), а согласие, без которого недоступна сама услуга, суды склонны признавать вынужденным (88-17782/2025, компенсация 12 000 ₽)

Согласие по умолчанию с графой "не согласен" уязвимо

Принудительные согласия на проверку сведений, рекламу и обработку ПД в договоре оператора связи

Privacy Advocates

"СОГЛАСЕН, ЕСЛИ НЕ УКАЗАНО ДРУГОЕ" И КЛЕТКА "НЕ СОГЛАСЕН"

- **Проверка сведений**
  проверка сообщенных абонентом сведений по условиям договора
- **Зачет платежей**
  деньги по одному договору идут на долг по другому
- **Реклама оператора**
  рекламная информация и рассылки от оператора
- **Реклама третьих лиц**
  рекламная информация и рассылки от третьих лиц
- **Обработка ПД**
  обработка ПД по пп.3.3-3.6 условий
- **Сведения в кабинете**
  предоставление сведений в личном кабинете

Все шесть согласий считаются данными, пока абонент сам не отметит клетку **"не согласен"** рядом с каждым из них, то есть отказ требует действия, а согласие нет

ОЦЕНКА 2026

Почему конструкция уязвима

- согласие выводится из бездействия, а бездействие формой согласия быть не может (Роскомнадзор, 29.09.2022)
- с 01.09.2025 согласие оформляется отдельно от договора (ч.1 ст.9)
- выражать согласие за потребителя и формировать условия с изначальным согласием запрещает п.3.1 ст.16 ЗоЗПП
- практика по графе о несогласии разошлась: А40-172089/2018 за оператора (первая инстанция), А40-64096/2017 против (АС МО 01.02.2018)

Расчет цены полиса не оправдывает сбор паспортных данных

Два иска одной гражданки к страховщикам о сборе ПД на сайте для расчета ОСАГО

Privacy Advocates

Иск удовлетворен

СК "Согласие"

апелляционное определение Мосгорсуда от 04.04.2022 № 33-9501/22

для расчета стоимости ОСАГО сайт требовал ФИО, дату рождения, пол, паспорт и водительское удостоверение, а соглашение считало использование сайта согласием на обработку и передачу ПД для рекламы

- Мещанский суд в иске отказал, Мосгорсуд решение отменил и удовлетворил все требования
- объем признан избыточным, условие о согласии пользованием сайта исключено, перечень третьих лиц внесен

vs

В иске отказано

"Абсолют Страхование"

апелляционное определение Мосгорсуда от 30.11.2023 № 33-49093/2023

ПД истребованы в объеме, необходимом для расчета стоимости страхования ОСАГО

- решающим стал объем запрашиваемых сведений, а не сам факт сбора

Логика ст.16: сведения о цене раскрывают до сбора данных, а требование ПД лишь ради того, чтобы узнать цену, Роспотребнадзор считает нарушением п.4 ст.16 ЗоЗПП (вебинар 27.07.2023)

12.3

ПД детей

- Согласие подростка: три позиции и ни одной устойчивой
- Школа и детсад ведут ПД по закону, через обработчика и по согласию
- Публикация о ребенке проходит три фильтра, а не один
- Возраст пользователя проверяют по уровню риска, а не для галочки

Согласие подростка: три позиции и ни одной устойчивой

Как менялись устные позиции РКН по возрасту 14-18 лет и на что опираются письма и суды

Privacy Advocates

28.01.2022

РКН УСТНО

С 14 лет хватает согласия подростка

в пределах его дееспособности

31.01.2024

РКН УСТНО

До 18 лет подписывает представитель

кроме случаев, прямо предусмотренных законом

22.10.2025

РКН УСТНО

От 14 до 18 лет сам в рамках дееспособности

до 14 лет через законного представителя

14.08.2026

РКН УСТНО

Сам только в случаях ст.26 ГК

в остальных согласие дает законный представитель

позиция 1

Подросток сам в пределах ст.26 ГК

письма РКН от 30.03.2023 № 08-26424 и от 30.05.2024 № 08-192564, ЕСИА с 14 лет в пределах дееспособности (ПП № 977)

позиция 2

Всегда законный представитель

письмо Управления РКН по ЦФО от 02.05.2024, дело А70-2034/2017 о биометрии учащихся, дело 12-2573/2026 по ч.6 ст.9

позиция 3

Подросток с одобрением представителя

экспертная конструкция по аналогии со ст.26 и 175 ГК, прямой опоры в позициях РКН и судов нет

Опора: ч.6 ст.9 152-ФЗ написана для недееспособных (ст.29 ГК), но в деле 12-2573/2026 ее применили к подростку. По экспертному подходу детскую форму надежнее строить на ст.26 и 28 ГК и отраслевых нормах

Школа и детсад ведут ПД по закону, через обработчика и по согласию

Что школа и детский сад ведут без согласия, что через поручение и что только по отдельному согласию

Privacy Advocates

ПРОЦЕСС	ОСНОВАНИЕ	ГРАНИЦА
Прием, контингент, аттестация, документы об образовании	закон об образовании, п.2 ч.1 ст.6	копии паспортов обоих родителей и справки о доходах сверх отраслевой нормы избыточны
Всероссийская олимпиада	приказ Минпросвещения, п.2 ч.1 ст.6	письмо РКН от 07.12.2023 № 08-133024, публикация без согласия по ч.15 ст.10.1 - экспертный вывод
Госуслуга или выплата на ребенка	закон, п.4 ч.1 ст.6	отказ без согласия второго родителя неправомерен
Электронный журнал, облачная платформа	поручение с согласия представителя, если закон не дает иного	договор с перечнем действий и локализация, а сервис со своими целями уже получатель
Фото на сайте, конкурсы вне программы, биометрия	отдельное согласие	отказ родителя от добровольного блока не влияет на обучение

МИНЦИФРЫ, 28.08.2020

Три потока субъектов в одной школе

письмо № ЛБ-С-074-24059 делит данные учеников, родителей и работников по основаниям и объему

С 01.09.2025

Согласие не вшивают в заявление

согласие внутри заявления о зачислении не обособлено, его выносят в отдельную форму

Публикация о ребенке проходит три фильтра, а не один

Согласие на распространение, охрана изображения и частной жизни, отраслевые запреты и исключения

Privacy Advocates

1

Режим ПД

согласие на распространение по ст.10.1, за малолетнего его дает представитель. Поля для него в форме по приказу РКН № 18 нет, его добавляют, это спорно

2

Изображение и частная жизнь

ст.152.1 и 152.2 ГК действуют параллельно с 152-ФЗ, и снятие одного режима не снимает другой

3

Отраслевые запреты

редакция СМИ не раскрывает подростка-правонарушителя без согласия его и представителя, а пострадавшего только ради защиты прав (ст.41 закона о СМИ)

РЕКОМЕНДУЕТСЯ СВЕРХ СОГЛАСИЯ

не публиковать сведения об усыновлении, здоровье и трудной ситуации, не полагаться на скрытое имя при школе, классе и фото, дать канал отзыва и удаления

СПОРНО

Открыто не значит общедоступно

по экспертному подходу выложенное в сеть фото ребенка не основание для профилирования, устные позиции РКН 28.01.2022 и 14.08.2026 расходятся

Исключение: сведения о доходах детей служащие представляют по ст.8 закона о противодействии коррупции без согласия (п.2 ч.1 ст.6), а публикуют их только в объеме и на сайтах по антикоррупционным актам

Возраст пользователя проверяют по уровню риска, а не для галочки

Прямой обязанности нет, она следует из правил о согласии: барьер с журналом, ЕСИА, профили и порог 18+

Privacy Advocates

Низкий риск

- малый объем данных и низкая вероятность вреда
- возрастной барьер с сохранением выбора
- журнал с датой, временем, выбором и сессией, без него отметка не доказывает возраст

vs

Высокий риск

- спецкатегории, биометрия, публикация, профилирование, ТПД
- упрощенная авторизация или ЕСИА, где с 14 лет в пределах дееспособности согласие подключенным организациям дает подросток или представитель (ПП № 977)

РЕСУРС 18+

Порог подкрепляют уничтожением

детские данные перестают обрабатывать в течение 3 рабочих дней и уничтожают не позднее 10 (ч.3 ст.21), иначе порог доказывает осведомленность о риске

ДЕТСКИЙ ПРОФИЛЬ

Возраст для доступа, а не для маркетинга

возраст для фильтра по 436-ФЗ не берут в рекомендации, а родительский контроль, по КС (2-П), собирает сведения о частной жизни ребенка, но ради безопасности не противоправен

Зарубежные сервисы: зарубежные обучающие и игровые платформы с 01.07.2025 упираются в ч.5 ст.18, механизм для них спорен, а риск несет встроивший их оператор

13

Маркетинг и данные

Профилирование, рассылки и данные в цифровом бизнесе

13.1 Профилирование и прямой маркетинг

13.2 Данные в цифровом бизнесе

13.3 Саморегулирование, платформы и экосистемы

Раздел на сайте
privacy-advocates.ru/pd/mrk

13.1

Профилирование и прямой маркетинг

Мониторинг

- Профилирование оценивает человека, таргетинг его использует
- Прямой маркетинг допустим только с предварительным согласием
- Одно маркетинговое сообщение проверяют по трем законам
- Рекламное согласие зависит от способа сбора и записи о нем

Профилирование оценивает человека, таргетинг его использует

Две операции маркетинговой аналитики и правовые основания для них в 2026 году

Privacy Advocates

Профилирование

Оценка личных аспектов

любая форма автоматической обработки ПД для оценки определенных личных аспектов человека, в частности для анализа или предугадывания результативности в работе, экономического положения, здоровья, предпочтений, интересов, надежности, поведения и перемещений

Таргетирование

Доставка предложения

использование результатов профилирования для информирования, доставки персональных предложений и рекламных сообщений через различные каналы в интересах оператора и третьих лиц

Определение

в 152-ФЗ профилирования нет, формулировка восходит к ст.4 GDPR, а ст.16 152-ФЗ ограничивает лишь решения, основанные исключительно на автоматизированной обработке

Основание

адресная реклама, скоринг и рекомендательные алгоритмы требуют собственного основания по ст.6, а при прямых контактах в целях продвижения - согласия по ч.1 ст.15

Вред

профилирование создает о человеке новую информацию без его ведома и ведет к негативным решениям о нем

Повестка

в 2026 году обсуждают отраслевые стандарты вместо согласия и платформу управления согласиями

Прямой маркетинг допустим только с предварительным согласием

Ст.15 152-ФЗ: специальное правило с презумпцией отсутствия согласия и правом на отказ

Privacy Advocates

СТ.15 152-ФЗ

Норма

- обработка ПД в целях продвижения товаров, работ и услуг путем прямых контактов с потенциальным потребителем с помощью средств связи, а также для политической агитации допускается **только с предварительного согласия** субъекта (ч.1)
- обработка признается осуществляемой без согласия, **если оператор не докажет**, что оно получено (ч.1)
- по требованию субъекта оператор обязан **немедленно прекратить** такую обработку (ч.2)

ЧТО ИЗ ЭТОГО СЛЕДУЕТ В 2026 ГОДУ

Договор и интерес не помогают

маркетинговая цель не выводится ни из договора с адресатом, ни из законного интереса оператора

Форма любая, но доказуемая

письменная форма не нужна, а отметка, запись звонка или код подтверждения работают при журнале согласий

Сервис или реклама

сообщение во исполнение договора рекламой не является, но промоблок переводит его в рекламу целиком

Отзыв останавливает рассылку

отзыв согласия по ст.15 обязывает прекратить и рекламную коммуникацию

Где ловят: по устной позиции Роскомнадзора (14.08.2026) крупные операторы чаще всего нарушают ч.1 ст.15 на рассылках по электронной почте. Адрес почты сам по себе регулятор отнес к ПД письмом от 08.08.2024 № 08-329520, хотя суды этот критерий отвергали (раздел 05)

Одно маркетинговое сообщение проверяют по трем законам

Ст.18 закона о рекламе в связке со ст.15 152-ФЗ и законом о связи

Privacy Advocates

НОРМА	ЧТО ТРЕБУЕТ	КТО ДОКАЗЫВАЕТ	КАК ПРЕКРАЩАЕТСЯ
ч.1 ст.15 152-ФЗ	предварительное согласие субъекта на обработку в целях продвижения прямыми контактами	оператор ПД	немедленно по требованию субъекта
ч.1 ст.18 закона о рекламе	предварительное согласие абонента или адресата на рекламу по сетям электросвязи	распространитель рекламы	немедленно по требованию адресата
ч.2 ст.18 закона о рекламе	**запрет автодозвона и авторассылки**	презумпции нет	согласием не легализуется
п.1 ст.44.1 закона о связи	согласие абонента на рассылку по подвижной связи	заказчик или оператор связи	отказ у оператора связи со следующего дня
ст.44.1-1 закона о связи	согласие на массовые вызовы с 01.09.2025 и договор с оператором абонента	заказчик вызовов	безусловный отказ у оператора связи

Вывод: согласия трех режимов друг друга не заменяют, а согласие на обработку ПД при регистрации рекламным согласием не является

Рекламное согласие зависит от способа сбора и записи о нем

Четыре модели сбора, три требования к фиксации и отдельная отметка по каждому каналу связи

Privacy Advocates

МОДЕЛЬ	РИСК	ПРАКТИКА
Двойное активное подтверждение	минимальный	пустая отметка и код или ссылка, негативной практики нет
Однократное активное	низкий	пустая отметка без верификации, однозначность соблюдена
Преднастроенная отметка	спорный	суда нет, УФАС Москвы 24.09.2026 признало ненадлежащей
Отметка о несогласии	не однозначна	молчание не согласие, исходы по операторам связи разошлись

ТРИ ТРЕБОВАНИЯ К ФИКСАЦИИ

1. **Адресат**
   конкретный рекламораспространитель, а не будущие партнеры
2. **Отдельность**
   формулировка о рекламе не растворена в политике
3. **Запись**
   время, текст показанной надписи и идентификатор субъекта

Каналы и номер: согласие дают отметкой по каждому каналу: звонки, СМС, почта, мессенджеры, push. Номер подтверждают кодом, иначе журнал доказывает лишь, что кто-то ввел цифры

Массовые вызовы требуют согласия, договоров и маркировки

Режим ст.44.1-1 закона о связи с 01.09.2025 и его изменения 2026-2027 годов

Схема массовых вызовов
скачать

Privacy Advocates

1 Отсечь запрещенное

автодозвон для рекламы запрещен ч.2 ст.18 закона о рекламе и согласием не легализуется

2 Оценить массовость

порог задает антифрод-политика оператора связи, поэтому кампанию планируют от худшего сценария

3 Собрать согласие

предварительное, однозначно идентифицирующее абонента и именно на вызовы, доказывает заказчик

4 Заключить договоры

с каждым оператором, абонентам которого предназначены вызовы

5 Оформить маркировку

договор об отображении: наименование и категория вызова до 32 символов (ПП от 28.08.2025 № 1300)

- оператор связи вправе не пропускать вызовы без согласия и запросить его подтверждение у заказчика (письмо Минцифры от 29.12.2025 № П12-130083)
- отказ абонента у оператора неизбирателен и отключает все массовые вызовы, кроме вызовов органов и организаций из перечня
- операторы объявили блокировку немаркированных вызовов с 15.10.2026, Минцифры 14.10.2026 просило до ноября не блокировать банки, для немассовых вызовов это спорно
- с 01.03.2027 изъяты информирующие вызовы по обязанности из актов и вызовы банков по договору с абонентом (210-ФЗ от 26.06.2026)

Детям до 14 лет рекламу по связи шлют с согласия родителя

Прямой маркетинг, профилирование детей и проект запрета СМС на детские номера

Privacy Advocates

1

Прямые контакты

по ч.1 ст.15 только с предварительного согласия, за малолетнего его дает законный представитель. Таргетированную рекламу без прямых контактов норма не охватывает

2

Профилирование

особого запрета для детей нет: ст.16 запрещает исключительно автоматизированные решения с юридическими последствиями для любого субъекта, а детский профиль повышает оценку вреда

3

Проект Минцифры

запрет СМС на номера, переданные детям, включая коды входа, исключения для п.3 ст.44.1 закона о связи, Банка России, НСПК и ГИС. На 30.09.2026 не принят

Что делать: детский сервис заранее строит вход без СМС-кода, а маркетинг ведет по отдельному согласию представителя с раздельным отзывом

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OPR-014	Виды ПД по способам их получения	05 Определение ПД

13.2

Данные в цифровом бизнесе

- Курс 4 - Работа с данными

Подключенный автомобиль генерирует до 4 Тб данных в день

Рынок Автонет: телематика, городская мобильность и логистика

Privacy Advocates

ТРИ НАПРАВЛЕНИЯ ЭКОСИСТЕМЫ РЫНКА АВТОНЕТ

- телематические транспортные и информационные системы
- интеллектуальная городская мобильность
- транспортно-логистические услуги

Данные охватывают все от местоположения по ГНСС-приемнику до состояния машины и водителя, а полностью оснащенная машина выдает **около 4 Тб в день**

20-60 Мб/с

Камеры

главный поток для беспилотника

10-70 Мб/с

Лидары

сканирование окружения

до 10 Кб/с

Радары

ультразвук 10-100 Кбайт/с

около 50 Кб/с

GPS

местоположение машины

Для маркетинга: геолокация и данные о водителе становятся ПД в связке с человеком, а предложение под текущее местоположение требует согласия по ч.1 ст.15 152-ФЗ и, при доставке по сетям электросвязи, по ч.1 ст.18 закона о рекламе

Программатик покупает не трафик, а конкретных пользователей

Экосистема programmatic: закупка рекламы в реальном времени через аукцион

Privacy Advocates

Программатик - способ закупки трафика в режиме реального времени через интерфейсы рекламных систем, который позволяет покупать не весь массив трафика или контента, а **конкретных пользователей**

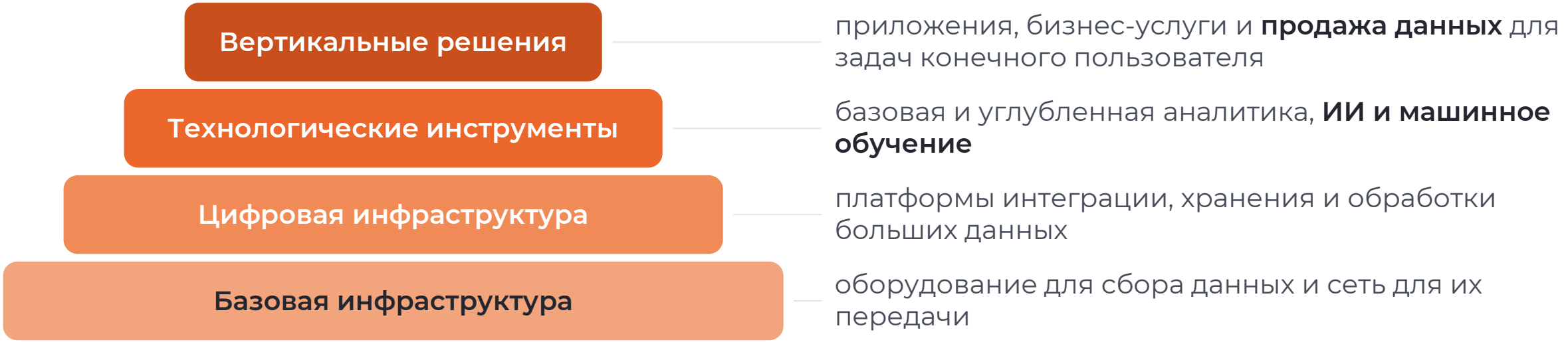
1. **Посетитель**
   заходит на сайт или в приложение рекламной площадки
2. **Рекламная площадка**
   передает показ на продажу
3. **SSP**
   платформа продавца выставляет показ на аукцион
4. **DSP и DMP**
   платформы покупателей делают запрос, участвуют в аукционе и ставке по данным о пользователе
5. **Рекламное агентство**
   трейдинг-деск (TD/ATD) управляет закупкой для рекламодателя

Правовой слой: баннер на стороннем ресурсе рекламного согласия адресата не требует, поскольку прямого контакта нет, но обработка идентификаторов пользователя для таргетинга нуждается в основании по ч.1 ст.6 152-ФЗ

Аналитика больших данных строится на четырех уровнях

Ключевые элементы по отраслевой Стратегии АБД, срок которой истек в 2024 году

Privacy Advocates



ГЕНЕРАЦИЯ ДАННЫХ

- личная активность и операции
- движение транспортных средств
- производственные процессы

Напряжение с 152-ФЗ: ценность больших данных извлекается объединением наборов, собранных для разных задач, что конфликтует с целевым ограничением и сроками хранения, поэтому маршрут выбирают заранее: новая цель, обезличивание или проверка совместимости

13.3

Саморегулирование, платформы и экосистемы

- Кодексы этики данных задают ориентиры, а не обязанности
- Отказ от рекламы должен останавливать всю цепочку рассылки
- Экосистема объединяет продукты вокруг потребностей клиента
- Пункт о продуктах группы компаний затрагивает четыре режима

Кодексы этики данных задают ориентиры, а не обязанности

Кодекс Роскомнадзора о работе в интернете и Кодекс этики использования данных АБД и ИРИ

Privacy Advocates

Роскомнадзор

Кодекс этической деятельности в сети Интернет

pd.rkn.gov.ru/code

- внимание граждан, государства, общества и бизнеса к безопасному интернету и защите прав субъектов ПД, информированность об угрозах частной жизни
- новые исследования функционирования интернета и цифрового суверенитета и их внедрение в практику
- освещение положительного опыта соблюдения прав и свобод человека в сети

vs

АБД и ИРИ

Кодекс этики использования данных

csr.ru/ru/ethics

отраслевой акт саморегулирования, фиксирующий основные принципы работы с данными

- закрепить принципы взаимодействия государства, граждан и бизнеса
- регламентировать универсальные правила допустимого поведения для всего профессионального сообщества

Статус: 152-ФЗ кодексов поведения не знает, поэтому присоединение к кодексу служит каркасом внутренних решений и доводом о добросовестности, но не заменяет требований закона в споре с регулятором

Отказ от рекламы должен останавливать всю цепочку рассылки

Privacy Advocates

ЦИКЛ С МАРКЕТИНГОВЫМ ПОСРЕДНИКОМ

1. **Согласие**
   пользователь дает согласие сервису
2. **Поручение**
   сервис поручает посреднику маркетинговые коммуникации
3. **Коммуникации**
   посредник направляет пользователю маркетинговые сообщения
4. **Отказ и запрет**
   пользователь отказывается от коммуникаций, а сервис запрещает их посреднику

КОММУНИКАЦИИ ПО УЖЕ ОКАЗЫВАЕМЫМ УСЛУГАМ

1. **Запрос**
   сервис запрашивает у клиента согласие на рекламу
2. **Явное согласие**
   только оно открывает рекламную коммуникацию
3. **Нет согласия**
   отсутствие согласия ведет к прекращению рекламной коммуникации

В 2026 году: отписка доступна с первого сообщения и работает по всем каналам сразу, согласие дается конкретному распространителю, а отказ абонента у оператора связи и требование по ч.2 ст.15 152-ФЗ - разные механизмы с разными исполнителями

Экосистема объединяет продукты вокруг потребностей клиента

Цифровые платформы и экосистемы: определения и масштаб тренда

Privacy Advocates

Цифровая платформа

бизнес-модель, позволяющая потребителям и поставщикам связываться онлайн для обмена продуктами, услугами и информацией, включая собственные

Цифровая экосистема

клиентоцентричная бизнес-модель, объединяющая две и более группы продуктов, услуг и информации для удовлетворения конечных потребностей клиентов

Платформы выросли из офлайна - торговых центров, вокзалов, аэропортов, а экосистемы стали их следующей фазой. Клиенты выбирают экосистемы за удобство, выбор и цену, Amazon строит свою более 25 лет

30%

Электронная коммерция

мирового рынка занимают национальные экосистемы США и Китая

75%

Блокчейн

патентов приходится на США и Китай

50%

Интернет вещей

рынка у США и Китая

75%

Облака

рынка облачных вычислений у США и Китая

Пункт о продуктах группы компаний затрагивает четыре режима

Согласие на продукты компаний группы: ПД, добровольность, реклама и навязывание

Privacy Advocates

01

Прямой маркетинг

информирование о продуктах компаний группы требует согласия по ч.1 ст.15 152-ФЗ, а договор его не заменяет

02

Добровольность

согласие, подписанное как часть договора, не свободно, а с 01.09.2025 его оформляют отдельно (ч.1 ст.9)

03

Реклама

согласие дается конкретному распространителю, и абстрактные партнеры без перечня его не получают (п.15 постановления Пленума ВАС № 58)

04

Навязывание

обусловливание договора заключением иных договоров недопустимо (подп.5 п.2 ст.16 ЗоЗПП)

- назовите компании группы поименно или дайте ссылку на актуализируемый перечень с архивом редакций
- храните признак, какой компании дано согласие: Роскомнадзор (14.08.2026) не допускает одно согласие нескольким равноправным операторам
- проверьте, что отказ от партнерского блока технически возможен и не блокирует оформление основного продукта
- при конфликте статусов в системах группы побеждает отказ, а отзыв из любой точки уходит всем отправителям

Вывод: устранение одного дефекта остальные не снимает, поэтому экосистемный пункт разбирают по всем четырем основаниям сразу

14

Распространение ПД

Когда раскрытие ПД становится распространением и как его легализовать

14.1 Проблематика распространения

14.2 Способы легализации и позиции 2021-2026

14.3 Согласие на распространение

14.4 Практика и рекомендации

Раздел на сайте
privacy-advocates.ru/pd/rsp

14.1

Проблематика распространения

- ПД могут подпадать сразу под несколько режимов информации
- 519-ФЗ отменил общедоступность как основание обработки
- Распространение - раскрытие неопределенному кругу лиц
- 519-ФЗ породил новые понятия и конкуренцию норм

ПД могут подпадать сразу под несколько режимов информации

Диаграмма Эйлера: где ПД пересекаются с ограниченным доступом и общедоступной информацией

Privacy Advocates

ОГРАНИЧЕННЫЙ ДОСТУП

Информация ограниченного доступа

ч.2 ст.5 и ст.9 149-ФЗ

- охраняемые законом тайны, ч.3-8 ст.9 149-ФЗ
- иная информация ограниченного доступа, ст.15.2, 15.3, 15.5, 15.6 149-ФЗ
- биометрические ПД, ст.11 152-ФЗ и 572-ФЗ

ПД В ЗОНЕ ОБЩЕДОСТУПНОЙ ИНФОРМАЦИИ, Ч.2 СТ.5 И СТ.7 149-ФЗ

РЕЖИМ ПД	НОРМА 152-ФЗ
опубликованы в рамках журналистики, СМИ, научной, литературной и иной творческой деятельности	п.8 ч.1 ст.6
опубликованы или раскрыты на основании федерального закона	п.11 ч.1 ст.6
включены в общедоступные источники с согласия субъекта	ст.8
разрешены субъектом для распространения	ч.1 ст.10.1
раскрыты неопределенному кругу лиц самим субъектом	ч.2 ст.10.1
раскрыты вследствие правонарушения, преступления или непреодолимой силы	ч.3 ст.10.1

Вывод: ПД в целом (ч.9 ст.9 149-ФЗ и 152-ФЗ) пересекают обе зоны, и у каждого общедоступного режима своя норма 152-ФЗ. Рядом действуют режимы общеизвестных сведений (ст.7), информации, доступ к которой не может быть ограничен (ст.8), и открытых данных (ч.4 ст.7 149-ФЗ)

519-ФЗ отменил общедоступность как основание обработки

Закон от 30.12.2020 № 519-ФЗ: новые правила для ПД, разрешенных для распространения

Privacy Advocates

519-ФЗ ОТ 30.12.2020

Общедоступность больше не основание

П.10 ч.1 ст.6 152-ФЗ утратил силу. Доступность ПД неограниченному кругу лиц сама по себе не делает обработку законной и не заменяет согласие.
По **ч.2 ст.10.1** каждое лицо, которое распространяет или иначе обрабатывает ПД, разрешенные для распространения, обязано иметь свое основание из ч.1 ст.6

НОВЫЕ ПРАВОМОЧИЯ СУБЪЕКТА ПД

- определить конкретные распространяемые ПД по каждой категории данных в согласии
- запретить оператору передачу распространяемых ПД неограниченному кругу лиц, кроме предоставления доступа
- запретить неограниченному кругу лиц обработку распространяемых ПД, кроме получения доступа, или установить ее условия
- по первому требованию прекратить передачу (распространение, предоставление, доступ) своих ПД любым лицом

Парадокс: по букве ч.2 ст.10.1 основание нужно даже для простого доступа к распространенным ПД

Распространение - раскрытие неопределенному кругу лиц

Дефиниции 152-ФЗ, ориентиры для понятия неопределенного круга и вывод для квалификации

Privacy Advocates

152-ФЗ, ст.3

Дефиниции закона

- **п.1.1** ПД, разрешенные для распространения - доступ неограниченного круга лиц к ним субъект предоставил согласием по 152-ФЗ
- **п.5** распространение - действия, направленные на раскрытие ПД неопределенному кругу лиц

Ориентиры

Неопределенный круг лиц

- **ВС РФ, обзор за I квартал 2004 г.** - круг, который нельзя индивидуализировать, привлечь в процесс, указать в решении и решить вопрос о правах каждого
- **ФНС, письмо от 25.04.2007 № ШТ-6-03/348@** - лица, которых нельзя заранее определить как получателей рекламы и сторону правоотношения

ВЫВОД РА

Распространение есть при любом из условий

- нет действий по фактическому ограничению доступа к ПД
- нельзя достоверно установить круг лиц с правом доступа к ПД в момент или период

РОСКОМНАДЗОР

Предоставление, а не распространение

- табличка с ФИО и должностью на двери кабинета, ведь посетители - определенный круг лиц (Ю. Контемиров, день открытых дверей 28.01.2022)
- интранет-справочник с рабочими контактами работников (письмо Роскомнадзора 2026 года)

519-ФЗ породил новые понятия и конкуренцию норм

Проблематика 1/2: терминология, форма согласия, общедоступные источники и посредники

Privacy Advocates

1 Новые понятия

волеизъявление названо "разрешением", рядом с прежним "неопределенным" кругом лиц появился "неограниченный", а ПД, сделанные общедоступными субъектом, заменены ПД, разрешенными для распространения

2 Закрытый доступ

по позиции Роскомнадзора, если оператор может разумно определить или ограничить круг лиц с доступом к ПД, например через предварительную регистрацию на сайте, это не распространение

3 Форма согласия

требования ч.4 ст.9 к письменной форме к согласию на распространение не применяются, содержание задает Роскомнадзор. Согласие дается оператору непосредственно или через информационную систему Роскомнадзора

4 Конкуренция норм

ст.10.1 и ч.4 ст.9 сталкиваются при включении ПД в общедоступные источники (ст.8) и при согласии работника на распространение. Минцифры и Роскомнадзор считают, что ст.10.1 к общедоступным источникам не применяется

5 Непосредственность

согласие от представителя можно обосновать общей нормой ч.1 ст.9, но законность сбора согласий иными лицами, например обработчиком по поручению, под вопросом

6 Переход

519-ФЗ вступил в силу 01.03.2021, кроме положений об информационной системе Роскомнадзора. Согласие получают у субъектов, вступивших во взаимодействие с оператором с этой даты

Роскомнадзор: закон обратной силы не имеет, поэтому согласие по приказу № 18 нужно для распространения, начатого с 01.03.2021

Запреты и требования субъекта - вызов для оператора

Проблематика 2/2: ч.5, 10, 12 и 14 ст.10.1 152-ФЗ на практике

Privacy Advocates

Ч.5 - СОМНЕНИЯ ТРАКТУЮТСЯ ПРОТИВ ОПЕРАТОРА

- чек-бокс, которым субъект подтверждает отсутствие запретов и условий
- поле для описания запретов и условий, можно с набором типовых формулировок

Учет условий субъектов в процессах - большой организационный и ресурсный вызов, а субъект получает простор для злоупотребления правом

Ч.10 - ЗА 3 РАБОЧИХ ДНЯ ОПУБЛИКОВАТЬ УСЛОВИЯ

оператор и его контакты | **ожидаемая аудитория**

цель и запрет иных целей | **разрешенные действия**

разрешенные способы | **срок доступа**

? Что делать, если между согласием и публикацией больше 3 рабочих дней?

Закон ответа не дает. Как довести разные условия субъектов до читателей списка, опубликованного единым блоком, тоже не решено

? По ч.12 прекратить передачу "в любое время" значит немедленно?

Согласие прекращается с момента поступления требования (ч.13). Безопасно прекращать передачу сразу, а 3 рабочих дня ч.14 считать внешним пределом

? По ч.14 как "любое лицо" идентифицирует субъекта?

Механизм проверки полномочий заявителя у лица, не инициировавшего распространение, закон не задает

14.2

Способы легализации и позиции 2021-2026

- Сбор распространенных ПД граждан РФ требует основания и баз в РФ
- Монополия согласия на распространение спорна
- Минцифры в 2021 году: согласие - единственное основание
- Общедоступный источник ПД ведут без согласия по ст.10.1

Сбор распространенных ПД граждан РФ требует основания и баз в РФ

Две задачи получателя: выбрать правовое основание и соблюсти ч.5 ст.18 152-ФЗ

Privacy Advocates

ТРУДНОСТИ ВЫБОРА И ОБЕСПЕЧЕНИЯ ОСНОВАНИЯ

01

Согласие

субъекта на обработку его ПД

02

Закон

функции, полномочия и обязанности, возложенные на оператора законодательством

03

Договор

стороной, выгодоприобретателем или поручителем по которому является субъект

04

Законный интерес

права и законные интересы оператора или третьих лиц, см. рекомендации RPPA

ЛОКАЛИЗАЦИЯ, Ч.5 СТ.18

Базы на территории РФ

При сборе ПД, в том числе через Интернет, запись, систематизация, накопление, хранение, уточнение и извлечение ПД граждан РФ ведутся с использованием баз данных в РФ

- **Особенность**: новые ПД, полученные анализом данных, ранее собранных в российские базы и переданных за рубеж, можно получать в зарубежных базах без предварительной локализации

Монополия согласия на распространение спорна

Доводы за и против того, что согласие по ст.10.1 - единственное основание распространения

Privacy Advocates

За

Согласие исключительно

- дефиниция в п.1.1 ст.3 прямо называет согласие субъекта квалифицирующим признаком, Минцифры в письме от 21.12.2021 считает его единственным основанием
- ч.15 ст.10.1 знает одно исключение - функции органов власти, местного самоуправления и подведомственных организаций, ему отвечают п.4 и отчасти п.11 ч.1 ст.6
- пояснительная записка к 519-ФЗ: согласие - исключительное основание обработки ПД, сделанных общедоступными, кроме государственных, общественных и иных публичных интересов
- по словам М. Вагнера на дне открытых дверей Роскомнадзора 28.01.2022, распространение возможно только через согласие, а договор и пользовательское соглашение его не заменяют

vs

Против

Возможны иные основания

- чч.2-3 ст.10.1 требуют доказать законность последующего распространения, что косвенно отсылает к пп.2-9.1 и 11 ч.1 ст.6
- согласие не годится, когда распространение неразрывно связано с предметом возмездного договора или раскрытие по закону обязательно не для органов власти
- по судебной практике 2023 года согласие на распространение - частный случай согласия на обработку (п.1 ч.1 ст.6)
- в мае 2024 года письмо Роскомнадзора № 08-166301 допустило распространение и по иным основаниям ч.1 ст.6, устные позиции остаются строже

Минцифры в 2021 году: согласие - единственное основание

Письмо Минцифры от 21.12.2021: согласие по ст.10.1 легитимирует и оператора, и третьих лиц

Privacy Advocates

> Единственным правовым основанием, которое свидетельствует о том, что субъект персональных данных разрешил распространять персональные данные, является согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения

Письмо Минцифры от 21.12.2021, ответ на письмо от 26.11.2021 № 442-исх/6091

ТАКЖЕ В ПИСЬМЕ

то же согласие - единственное основание обработки ПД любыми третьими лицами, если субъект разрешил оператору их распространять

ВОПРОС РА

как это соотносится с чч.2 и 3 ст.10.1, где доказательства законности последующего распространения или иной обработки не ограничены согласием?

Что дальше: в 2023-2024 годах суды, Минцифры и Роскомнадзор от этой позиции отошли, см. следующие слайды

Общедоступный источник ПД ведут без согласия по ст.10.1

Минцифры [2021]: включение в источник по ст.8 требует письменного согласия по ч.4 ст.9

Privacy Advocates

1. **Отдельное согласие**

   согласие на распространение оформляется отдельно от иных согласий (ч.1 ст.10.1), его содержание задает приказ Роскомнадзора от 24.02.2021 № 18

2. **Изъятие для власти**

   ст.10.1 не применяется к функциям органов исполнительной власти и местного самоуправления (ч.15). Иные операторы распространяют ПД только при отдельном согласии

3. **Общедоступные источники**

   ПД включаются в справочники, адресные книги и иные источники с письменного согласия субъекта (ч.1 ст.8), требования к форме - ч.4 ст.9

4. **Форма согласия**

   при разработке формы согласия на распространение целесообразно руководствоваться приказом № 18

ВЫВОД РА

Два согласия для двух режимов

- косвенно заявлена необходимость отдельного согласия на распространение даже при наличии иных оснований по ч.1 ст.6
- согласие на включение ПД в общедоступный источник в целях информационного обеспечения соответствует ч.4 ст.9, а не приказу № 18

Общедоступный источник служит только информированию

Минцифры [2025]: письмо от 23.03.2025 № П25-7197-ОГ и признаки источника по ст.8 152-ФЗ

Privacy Advocates

Информационный ресурс

напрямую не влияет на квалификацию обработки после отмены п.10 ч.1 ст.6

Одна цель

создается только для информационного обеспечения

Письменное согласие

наполняется с письменного согласия субъекта, отдельного от иных согласий

Сообщенные субъектом

состоит из ПД, сообщенных субъектом, иных ПД в теории нет

Воля субъекта

субъект вправе требовать незамедлительно прекратить обработку своих ПД

Любой круг

открыт группе, например персоналу, или всем, и тогда конкурирует со ст.10.1

Минцифры: внутренние справочники организации для информационного обеспечения могут быть общедоступными источниками ПД с требованиями ст.8

СМИ распространяют ПД без согласия по ст.10.1

Роскомнадзор [2022]: письмо от 06.10.2022 № 08-90016 о публичных интересах

ПД в литературе
скачать

Privacy Advocates

1

Основания ст.6

обработка допускается с согласия субъекта или при иных основаниях пп.2-11 ч.1 ст.6 152-ФЗ

2

Журналистика

п.8 ч.1 ст.6 - для деятельности журналиста, законной деятельности СМИ, научной, литературной и иной творческой деятельности без нарушения прав субъекта

3

Ст.10.1 с 01.03.2021

519-ФЗ ввел особенности обработки ПД, разрешенных субъектом для распространения

4

Публичные интересы

по ч.11 ст.10.1 запреты и условия субъекта не действуют при обработке в государственных, общественных и иных публичных интересах

Вывод: если СМИ обрабатывает ПД в соответствии с ч.11 ст.10.1, согласие на распространение получать не требуется. Граница проходит по существу деятельности, и регистрация СМИ сама по себе изъятия не создает

С 2024 года согласие уже не единственное основание

Минцифры и Роскомнадзор [2024]: письма от 14.05.2024 и 15.05.2024

Privacy Advocates

Минцифры

Письмо от 14.05.2024 № П25-12029-ОГ

- случаи обработки без согласия перечислены в пп.2-11 ч.1 ст.6
- п.8 ч.1 ст.6 допускает обработку для журналистики, СМИ, науки, литературы и творчества без нарушения прав субъекта
- без согласия оператор обрабатывает ПД только при основаниях, установленных законодательством о ПД
- согласие на распространение оформляется отдельно от иных согласий

Роскомнадзор

Письмо от 15.05.2024 № 08-166301

- обработка по пп.2 и 11 ч.1 ст.6 без согласия относится к ПД по п.1 ст.3
- требования ст.10.1 применяются только к ПД, разрешенным субъектом для распространения
- распространение ПД, помимо пп.2 и 11 ч.1 ст.6, может быть предусмотрено и в иных случаях ч.1 ст.6

Но: устные позиции Роскомнадзора строже. При обработке по договору согласие по приказу № 18 все равно оформляют (М. Вагнер, 28.01.2022), а оператор без акта, предусматривающего публикацию, оформляет согласие на распространение (22.08.2025 и 14.08.2026)

КС РФ: СМИ вправе публиковать ПД врача без его согласия

Постановление Конституционного Суда РФ от 25.05.2021 № 22-П о сайте отзывов о врачах

Privacy Advocates

Исключения из правила о согласии (пп.7, 8 и 11 ч.1 ст.6 152-ФЗ) толкуются в свете **п.1 ст.152.2 ГК**: сбор и распространение сведений о частной жизни без согласия допустимы в государственных, общественных или иных публичных интересах и если сведения ранее стали общедоступными или раскрыты самим гражданином. Тот же подход в ст.49 и 57 Закона о СМИ

П.8 ч.1 ст.6 152-ФЗ конституционен

он допускает размещение сетевым изданием ПД медицинского работника, ранее размещенных по закону на официальном сайте медицинской организации, **вне зависимости от его согласия**

Фильтр отзывов

редакция не допускает оценок третьих лиц, не относящихся к профессиональной деятельности, и очевидно противоправных высказываний

Проверка по обращению

редакция в разумные сроки проверяет сведения, приостанавливая доступ к отзыву или помечая его спорный характер

Судебный запрет

при систематическом злоупотреблении суд может запретить распространение ПД работника и отзывов о нем

Суды: согласие по ст.10.1 - частный случай согласия

Дело СК "Арсеналъ" против Управления Роскомнадзора по ЦФО, № А40-139096/2022

Privacy Advocates

АС МОСКОВСКОГО ОКРУГА, 30.03.2023

Раскрытие по закону согласия не требует

Страховщик разместил на сайте ПД руководителей и участников общества во исполнение пп.2 п.6 ст.6 Закона об организации страхового дела. Управление требовало отдельного согласия на распространение.
Верховный Суд РФ определением от 21.07.2023 № 305-ЭС23-12160 отказал в передаче жалобы

КЛЮЧЕВЫЕ ВЫВОДЫ

- распространение ПД руководителей и участников ведется на основании пп.2 и 11 ч.1 ст.6 152-ФЗ, чтобы довести информацию до страхователей, застрахованных лиц, выгодоприобретателей и будущих клиентов
- ст.10.1 устанавливает порядок обработки ПД, разрешенных для распространения, и это частный случай обработки с согласия субъекта, что следует из названия и содержания статьи
- ни ст.10.1, ни иные нормы 152-ФЗ не обязывают оператора получать согласие на обработку во исполнение обязанностей по закону и требований о раскрытии

Следствие: лишнее согласие при обязательном раскрытии не добавляет правомерности, а создает впечатление, что отказ субъекта остановит раскрытие

14.3

Согласие на распространение

- Согласие на распространение: состав и границы
- Согласие на распространение содержит девять реквизитов
- Не у каждого способа распространения есть адрес ресурса
- Согласие на распространение оформляют отдельно от других

Согласие на распространение: состав и границы

Приказ РКН № 18, ст.10.1 152-ФЗ и позиции 2021-2026 годов

Privacy Advocates

Девять обязательных реквизитов

01	ФИО субъекта, без замены идентификатором
02	Контактная информация
03	Сведения об операторе
04	Цели обработки
05	Категории и перечень ПД
06	Условия и запреты субъекта по категориям
07	Условия передачи только по внутренней сети или без нее
08	Информационные ресурсы оператора (адреса)
09	Срок действия, лучше конкретный

КАК ДАЕТСЯ

Лично и адресно

Представитель по доверенности не предусмотрен (РКН, 02.12.2021), согласие легитимирует только тот оператор, которому дано

Непосредственно или через ИС РКН

Веб-форма, личный кабинет с ПЭП, бланк по почте, с 01.03.2022 и через ЕСИА. Молчание согласием не является

Прекращение по требованию

Требование к оператору действует сразу (чч.12-13 ст.10.1), иное обрабатывающее лицо исполняет его за 3 рабочих дня (ч.14)

Отдельное согласие не нужно

обязательное раскрытие по закону (п.11 ч.1 ст.6, письмо РКН от 15.05.2024, дело А40-139096/2022), журналистика и творчество (п.8), функции госорганов (ч.15 ст.10.1), сведения о педагогах и медработниках в объеме перечня

Спорно: иные основания

Письмо РКН 08-166301 (2024) и суд округа (2023) допускают иные основания ч.1 ст.6, но устно РКН требует согласие по приказу № 18 и при договоре (28.01.2022, 22.08.2025, 14.08.2026).

Согласие на распространение содержит девять реквизитов

Требования приказа Роскомнадзора от 24.02.2021 № 18 и позиции регулятора

Privacy Advocates

ПРИКАЗ РОСКОМНАДЗОРА ОТ 24.02.2021 № 18

1. фамилия, имя, отчество субъекта
2. контактная информация субъекта
3. сведения об операторе: организации, физлице или ИП
4. адреса ресурсов оператора: протокол, сервер, домен, каталог, имя файла страницы
5. цель или цели обработки
6. категории и перечень ПД, на обработку которых дается согласие
7. ПД, для которых субъект ставит условия и запреты, и сами условия и запреты
8. условия, при которых оператор может передавать ПД
9. срок действия согласия

? Добавить номер паспорта?

Нет, позиция Роскомнадзора

? Добавить дату и подпись?

Да, позиция Роскомнадзора

ПИСЬМО ОТ 17.09.2021 № 08-61656

Чужие ресурсы

Конструкция приказа предполагает размещение ПД на ресурсах оператора

- для чужих ресурсов согласие получает и их владелец
- третье лицо распространяет ПД от имени оператора на его ресурсах из согласия, соблюдая ч.3 ст.6 и ст.10.1

Не у каждого способа распространения есть адрес ресурса

Каналы раскрытия неограниченному кругу лиц, к которым плохо подходит п.4 приказа № 18

Privacy Advocates

СПОСОБЫ РАСПРОСТРАНЕНИЯ ПД

- сайты, порталы и мобильные приложения
- открытые каналы мессенджеров и соцсетей
- общедоступные стенды, в том числе электронные, киоски и терминалы
- потоковые трансляции и площадки видеоконференций
- издания и СМИ, где согласие не нужно в публичных интересах (ч.11 ст.10.1)
- радио- и телепередачи: эфир, кабель, записи, публичное исполнение
- рассылки любым потенциально заинтересованным лицам
- общедоступные справочные и адресные книги
- сообщение любым заинтересованным лицам
- надписи об ответственных за пожарную безопасность, ЧС и аптечки
- открытое ношение служебного пропуска на общедоступной территории
- реестры выданных и аннулированных сертификатов ключей ЭП

РОСКОМНАДЗОР, 28.01.2022

Нет сайта - ставим прочерк

Если ПД распространяются не через сайт, в поле об информационном ресурсе ставится прочерк, а остальные поля согласия заполняются

КОНЦЕПТ НА ПРАВАХ ШУТКИ

Доска позора из QR-кодов

На стенде вместо ФИО и фото разместить QR-коды. По комментарию должностного лица Роскомнадзора, по QR-коду невозможно установить личность, следовательно, данные не персональные

Согласие на распространение оформляют отдельно от других

Роскомнадзор (ЦФО) [2021]: правила оформления согласия на распространение

Privacy Advocates

НЕЛЬЗЯ

- разрабатывать и утверждать локальным актом собственную форму согласия, это законом не предусмотрено
- включать согласие на распространение в единое согласие на обработку или в текст договора

НЕ ТРЕБУЕТСЯ

- согласие на распространение для ПД из общедоступных источников по ст.8 152-ФЗ

ОБЯЗАТЕЛЬНО

- оформлять отдельно от согласий на поручение, на биометрию и специальные категории, на ТПД и на передачу ПД в трудовых отношениях
- указывать специальные категории и биометрию, только если есть письменное согласие на их обработку или иное основание по ст.10 и 11
- публиковать условия и запреты на ресурсах оператора или иным открытым способом, например на стенде
- считать согласие прекращенным полностью с момента поступления требования субъекта
- прежнее согласие до 01.03.2021 с правом распространения при требовании субъекта прекращать в части распространения

Обновление: на дне открытых дверей 14.08.2026 Роскомнадзор устно допустил собственную форму оператора в рамках приказа № 18, в том числе с заранее прописанными ограничениями

Условия и запреты в согласии устанавливает сам субъект

Минцифры [2021]: оператор не участвует в формулировании условий и запретов

Privacy Advocates

> Право установления в согласии [...] перечня устанавливаемых условий и запретов находится в компетенции субъекта персональных данных и не предусматривает участия оператора в его реализации

Письмо Минцифры от 21.12.2021, о пп.7-8 требований приказа № 18

ПРОБЛЕМЫ

1. произвольные запреты субъекта могут нарушить почти любой заранее продуманный процесс обработки
2. типовая форма на pd.rkn.gov.ru/soglasiya/maket предлагает только закрытые перечни условий и запретов
3. запрет участия оператора можно прочитать и как запрет рекомендаций субъекту по заполнению полей

Обновление: в 2026 году Роскомнадзор устно допустил заранее прописанные оператором ограничения. Безопасно предлагать их как отмечаемые варианты и сохранять поле для запретов самого субъекта (ч.9 ст.10.1)

Условия и запреты публикуются там же, где сами ПД

Роскомнадзор (ЦФО) [2021]: письмо от 02.07.2021 № 60836-02-11/77

Privacy Advocates

ПОЗИЦИЯ РОСКОМНАДЗОРА

Место публикации условий совпадает с местом ПД

"Опубликование информации об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных субъектом персональных данных для распространения, предполагается в том месте или на том Интернет-ресурсе, где будут размещены эти персональные данные оператором"

Повод

работодатель распространял ПД работников на стороннем ресурсе, цели и порядок в обращении не раскрыты

Рамка

с 01.03.2021 действует ст.10.1, а состав мер для исполнения обязанностей оператор определяет сам по ст.18.1

Срок

информацию об условиях и запретах публикуют в течение 3 рабочих дней после получения согласия, ч.10 ст.10.1

Следствие

условия и запреты публикуются в каждом месте размещения ПД отдельно, а не в одной точке ресурса

Согласие на распространение не дают по доверенности

Роскомнадзор [2021]: письма от 02.12.2021 № 08-81768 и от 29.12.2021 № 08-89152

Privacy Advocates

Доверенность

Представитель по доверенности не вправе

Письмо от 02.12.2021 № 08-81768

По п.1.1 ст.3 152-ФЗ доступ неограниченного круга лиц к ПД предоставляет сам субъект путем дачи согласия. Поэтому предоставление согласия представителем по доверенности не предусмотрено

- на практике такое согласие не принимают и предлагают субъекту выразить волю самому, в том числе через информационную систему Роскомнадзора

vs

Обучающиеся

Обучающийся дает согласие сам

Письмо от 29.12.2021 № 08-89152

Согласие на распространение предоставляется субъектом, поэтому обучающийся вправе дать его в объеме дееспособности по гражданскому законодательству

- без согласия обучающихся образовательная организация должна подтвердить иные основания из ч.1 ст.6

Важно: за малолетнего до 14 лет согласие, в том числе на распространение, дает законный представитель, а подросток 14-18 лет дает его сам (письмо Роскомнадзора от 30.03.2023 № 08-26424)

Одного согласия по ст.10.1 хватает и для изображения

Роскомнадзор (ЦФО) [2024]: письмо от 17.09.2024 № 73073-02-11/77 и ст.152.1 ГК

Privacy Advocates

Фото или видео гражданина публикуются на сайте с ФИО, должностью и местом работы. Нужно ли кроме согласия по ст.10.1 согласие по ст.152.1 ГК?

Одного согласия по ст.10.1 достаточно как правового основания распространения ПД

Можно ли включить в согласие по ст.10.1 текст согласия по ст.152.1 ГК?

Включать в одно согласие тексты по ст.10.1 и по ст.152.1 ГК не нужно

Когда согласие на распространение нужно вообще?

Только если организация планирует распространять ПД. Если не планирует, получать его не нужно

А органам власти?

Ст.10.1 не применяется к функциям госорганов, муниципальных органов и подведомственных им организаций (ч.15)

Также: Минцифры в 2024 году ответило так же, указав, что при согласии по приказу № 18 дополнительное согласие для той же цели по нормам ГК не требуется. Изображение при этом охраняется ст.152.1 ГК самостоятельно, поэтому изъятия проверяют по обоим режимам

Согласие работника на распространение оформляют по приказу № 18

Роскомнадзор [2025]: письмо от 19.06.2025 № 08-297178 о согласии через информационную систему

Privacy Advocates

Вопрос: правомерно ли распространять ПД работника по согласию на основании ч.6 ст.10.1 и приказа № 18, если работник дал его не в письменной форме по ст.88 ТК, а непосредственно работодателю через информационную систему?

1

Ч.1 ст.10.1

согласие оформляется отдельно от иных согласий, оператор дает субъекту определить перечень ПД по каждой категории

2

Ч.9 ст.9

требования к содержанию согласия на распространение устанавливает уполномоченный орган

3

Приказ № 18

требования утверждены приказом Роскомнадзора от 24.02.2021 № 18

4

Ответ

согласие должно соответствовать приказу № 18 и быть предоставлено в порядке ст.10.1

Цена ошибки: Роскомнадзор (22.10.2025) квалифицирует отсутствие согласия на распространение по ч.1 ст.13.11 КоАП, а нарушения его формы по ч.2 ст.13.11

Роскомнадзор проверяет согласия и запреты прямо на сайтах

Роскомнадзор [2026]: контрольное мероприятие без взаимодействия в Ульяновской области

Privacy Advocates

23.03.2026

ЗАДАНИЕ

Задание на мероприятие

руководитель Управления утвердил задание № 28-нд на контроль без взаимодействия с оператором

23-25.03.2026

АНАЛИЗ САЙТА

Наблюдение за соблюдением

пп.58-60 Положения о контроле за обработкой ПД (постановление Правительства от 29.06.2021 № 1046)

Выявлено

СТРАНИЦА САЙТА

Фото тренеров

указаний на согласия субъектов и сведений об условиях и запретах на обработку неограниченным кругом лиц нет

30.03.2026

ТРЕБОВАНИЕ

Основания не подтверждены

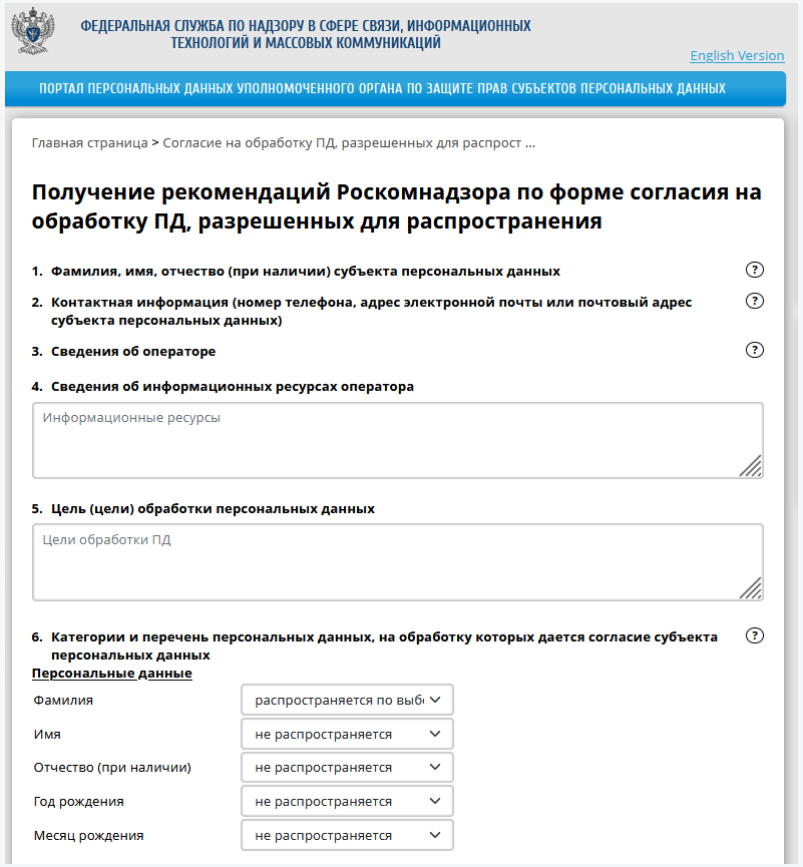
подтверждения правовых оснований распространения ПД тренеров на сайте нет

Вывод: нарушения ст.10.1 надзор находит дистанционно, ведь опубликованные ПД без согласия и без блока условий и запретов видны по самому сайту

Сервис Роскомнадзора подсказывает форму согласия

Рекомендательный сервис pd.rkn.gov.ru/soglasiya/maket и пояснения Роскомнадзора от 26.07.2021

Privacy Advocates


ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

English Version

ПОРТАЛ ПЕРСОНАЛЬНЫХ ДАННЫХ УПОЛНОМОЧЕННОГО ОРГАНА ПО ЗАЩИТЕ ПРАВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

Главная страница > Согласие на обработку ПД, разрешенных для распрост ...

Получение рекомендаций Роскомнадзора по форме согласия на обработку ПД, разрешенных для распространения

1. **Фамилия, имя, отчество (при наличии) субъекта персональных данных**
2. **Контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных)**
3. **Сведения об операторе**
4. **Сведения об информационных ресурсах оператора**

Информационные ресурсы

5. **Цель (цели) обработки персональных данных**

Цели обработки ПД

6. **Категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных**

Персональные данные

Фамилия	распространяется по выб
Имя	не распространяется
Отчество (при наличии)	не распространяется
Год рождения	не распространяется
Месяц рождения	не распространяется

РЕЖИМ ДЛЯ КАЖДОГО ВИДА ПД

не распространяется

распространяется обязательно

по выбору субъекта

ПОЯСНЕНИЯ К РЕЖИМУ "ОБЯЗАТЕЛЬНО"

Обязательное распространение по закону

указать реквизиты и наименование нормативного правового акта, который предусматривает обязательное распространение (опубликование) ПД

Договор

если правовым основанием распространения служит договор, стороной которого является субъект, в согласии указываются реквизиты договора: дата и номер

Заметим: сам регулятор в пояснениях к сервису называет договор правовым основанием распространения

14.4

Практика и рекомендации

- За телефон блогера на YouTube Google заплатил 60 тыс. ₽
- Страницу с ПД без согласия суд внес в реестр нарушителей
- Утечка ПД работников стала незаконным распространением
- Три вопроса до получения согласия на распространение

За телефон блогера на YouTube Google заплатил 60 тыс. ₽

Ч.5 ст.13.11 КоАП: неисполнение требования об уточнении, блокировании или уничтожении ПД

Privacy Advocates

60 тыс. ₽

Google, 2022

на YouTube без согласия опубликован телефон блогера. Он обратился в Роскомнадзор, тот составил протокол

50-90 тыс. ₽

Санкция ч.5

штраф для юридического лица, а при повторности по ч.5.1 от 300 до 500 тыс. ₽

50 тыс. ₽

Google, 2026

новый штраф по ч.5 ст.13.11, постановление от 18.03.2026 № 05-0216/422/2026 оставлено в силе 21.05.2026

Что наказывается

неисполнение требования субъекта или Роскомнадзора об уточнении, блокировании или уничтожении ПД

2025: YouTube и Telegram

штрафы по 80 тыс. ₽ по ч.5 ст.13.11 за неисполнение требований об удалении ПД, дела 05-0204/422/2025 и 05-0027/422/2025

Вывод: иностранная платформа, которая не удаляет опубликованные без согласия ПД по требованию, отвечает по ч.5 ст.13.11 КоАП

Страницу с ПД без согласия суд внес в реестр нарушителей

Мосгорсуд [2022]: апелляционное определение от 22.12.2022 № 33-46651/2022, Google LLC

Privacy Advocates

01

Публикация

на интернет-странице видеохостинга YouTube распространялись ПД гражданина

02

Незаконная деятельность

суд признал деятельность страницы незаконной и нарушающей права на неприкосновенность частной жизни, личную и семейную тайну

03

Нарушение 152-ФЗ

информация на странице признана обрабатываемой с нарушением законодательства о ПД, в том числе ст.10.1

04

Реестр

интернет-страница включена в Реестр нарушителей прав субъектов ПД

Практика: Роскомнадзор продолжает этот путь: в 2026 году Таганский районный суд удовлетворил его иски о незаконном распространении ПД по ч.1 ст.10.1, в том числе о дипфейке (дела 02-0901/2026 и 2-1452/2026, первая инстанция)

Утечка ПД работников стала незаконным распространением

Мировой судья, дело № 05-0470/456/2023 от 05.05.2023: ФГУП "ГРЧЦ" и ч.2 ст.13.11 КоАП

Privacy Advocates

30 тыс. ₽

МИРОВОЙ СУДЬЯ, 05.05.2023

Работодатель не обеспечил конфиденциальность

Из базы данных работников Центра в Интернет неограниченному кругу лиц попали ФИО, внутренние номера телефонов и адреса электронной почты работников. Письменного согласия работников на это не было

ЧТО УСТАНОВИЛ СУД

- ФГУП "ГРЧЦ" как работодатель нарушил ч.1 ст.6, ст.7, ч.4 ст.9, ч.1 ст.10.1 152-ФЗ и ст.88 ТК
- произошла неправомерная передача ПД (предоставление, распространение, доступ) неограниченному кругу лиц в сети Интернет
- содеянное образует состав ч.2 ст.13.11 КоАП, назначен штраф 30 тыс. ₽

Сегодня дороже: с 30.05.2025 штраф по ч.2 ст.13.11 для юридического лица 300-700 тыс. ₽, а утечка от 1 тыс. субъектов или 10 тыс. идентификаторов влечет от 3 млн ₽ по ч.12

Три вопроса до получения согласия на распространение

Алгоритм PA: уйти от квалификации, общедоступный источник или иное основание

Privacy Advocates

1. **Можно ли уйти от квалификации распространения?**
   определить определенный и ограниченный круг лиц, имеющих доступ к ПД

2. **Можно ли включить ПД в общедоступный источник?**
   по ст.8 152-ФЗ на основании письменного согласия, отвечающего ч.4 ст.9

3. **Можно ли опереться на иное основание?**
   обосновать распространение не согласием субъекта, а пп.2-9.1 и 11 ч.1 ст.6 152-ФЗ

ВОПРОС 1

Определенный круг - это два условия сразу

- **Установление допуска**: можно достоверно установить круг лиц, обладающих или обладавших правом доступа к ПД в определенный момент или период
- **Контроль доступа**: доступ к ПД фактически ограничен для лиц, не наделенных таким правом

Итог: если на все три вопроса ответ отрицательный, необходимо получить согласие на распространение по ст.10.1

Образец RPPA помогает оформить согласие по ст.10.1

Как дать согласие, из чего состоит образец и какой дисклеймер разместить рядом с ПД

Privacy Advocates

СПОСОБЫ ДАЧИ СОГЛАСИЯ, Ч.6 СТ.10.1

- непосредственно оператору через его информационную систему или в письменной форме
- через информационную систему Роскомнадзора по приказу от 21.06.2021 № 106

РАЗДЕЛЫ ОБРАЗЦА

оператор и цель | ПД: да или нет | ресурсы оператора | запрет передачи | запреты и условия обработки | передача по сети | срок | добровольность | права субъекта | порядок обращений | подтверждения

ДИСКЛЕЙМЕР, Ч.10 СТ.10.1

Размещается рядом с опубликованными ПД

"Размещенные на этой странице персональные данные распространяются с разрешения субъекта для цели [...]. Субъектом установлены следующие условия и запреты на обработку таких данных любыми лицами: [...]"

ОБРАЗЕЦ RPPA

rppa.ru/_media/analitika/srpd.docx

Форма с отметками ДА или НЕТ по каждому виду ПД, вариантами запретов и условий обработки и сносками о понятии распространения и о фото, не используемом как биометрия

15

Биометрические ПД

Когда сведения становятся биометрией, ЕБС и видеонаблюдение

15.1 Применение и риски биометрии

15.2 Квалификация биометрии

15.3 ЕБС и 572-ФЗ

15.4 СКУД, сценарии и встраивание в продукты

15.5 Видеонаблюдение

Раздел на сайте
privacy-advocates.ru/pd/bio

15.1

Применение и риски биометрии

- Стандарт знает 12 биометрических технологий и 10 сфер
- Биометрия раскрывает больше, чем лицо на снимке
- Распознавание лиц уже ищет людей в метро и в интернете

Стандарт знает 12 биометрических технологий и 10 сфер

ГОСТ Р 54412-2019 (ISO/IEC TR 24741:2018), разделы 6 и 7: обзор технологий и примеры применения

Privacy Advocates

Биометрия - это семейство технологий, а не одно распознавание лица. От модальности зависит правовой режим, поэтому выбор технологии делают вместе с юристом

ТЕХНОЛОГИИ РАСПОЗНАВАНИЯ, РАЗДЕЛ 6

- **изображение лица**
- **распознавание диктора**
- **изображение глаза**
- **отпечаток пальца и ладони**
- **геометрия кисти руки**
- **рисунок сосудистого русла**
- **динамика подписи**
- **работа на клавиатуре**
- **анализ запаха**
- **анализ ДНК**
- **кардиограмма**
- **походка и изображение тела**

ОБЛАСТИ ПРИМЕНЕНИЯ, РАЗДЕЛ 7

- физический контроль доступа
- логический контроль доступа
- учет рабочего времени и посещаемости
- отчетность
- электронная подпись
- государственные и гражданские услуги
- охрана границы
- правоохранительные органы
- проверки граждан
- кластеризация

Следствие: лицо и голос (выделены оранжевым) заводят в контур 572-ФЗ и ЕБС, а отпечаток, вены, радужка и поведенческие признаки остаются в режиме ст.11 152-ФЗ

Биометрия раскрывает больше, чем лицо на снимке

Кейсы: внешность по ДНК, отпечатки с фотографии, имя по лицу, ориентация по голосу, эхо уха

Privacy Advocates

Австралия, ДНК

Внешность по следам

Полиция применяет Massively Parallel Sequencing: по ДНК с места преступления прогнозирует пол, цвет глаз, страну происхождения, далее цвет волос, возраст и рост

Великобритания

Отпечатки со снимка

По фото в EncroChat, где рука держит кусок сыра, полиция Мерсисайда считала отпечатки пальцев автора. Итог - 13,5 года заключения за сбыт наркотиков

США, $2 млрд

Имя по лицу

Нейросеть по разработке The Mitre Corp угадывает имя человека из двух вариантов с точностью 72-80,5% без сличения с базами, а по имени подбирает лицо

Сиднейский университет

Ориентация по голосу

Слушатели по 60 записям точнее определяли ориентацию гомо- и гетеросексуальных мужчин, для бисексуальных метод оказался ненадежным

Apple, патент

Эхо уха

Ультразвуковые датчики AirPods распознают владельца по уникальному эху уха: в чужих ушах музыка остановится

Что это значит

Потенциал еще не режим

Режим ст.11 152-ФЗ включает цель установления личности. Выводы о здоровье или ориентации ведут в специальные категории ст.10

Распознавание лиц уже ищет людей в метро и в интернете

Кейсы массового распознавания: Сфера, Clearview AI, Google Street View, HR-система SAP

Privacy Advocates

Москва, транспорт

Сфера нашла 9007 разыскиваемых и 1324 пропавших

Система видеоаналитики работает с 1 сентября 2020 года, среди найденных пропавших 280 детей. Лицо превращается в биометрический ключ, доступ есть только у правоохранительных органов, об ошибках идентификации не сообщается

Clearview AI: около 30 млрд фото из соцсетей

без согласия владельцев, около миллиона запросов полиции США, в Майами около 450 раз в год

Google Street View нашел мафиози через 20 лет

Джоаккино Гаммино скрывался под Мадридом, пока его не сфотографировала машина Google Maps

HR-система SAP с термометрией и распознаванием

интеграция с HR, почтой и Telegram, слепки лиц названы обезличенными, хотя вектор обезличиванием не является

В России: поиск по изображению лица в собственной системе организации запрещен ст.15 572-ФЗ, а МВД и ФСБ получают сведения из ЕБС по мотивированному запросу

15.2

Квалификация биометрии

- Биометрию определяют три признака, и только вместе
- Лицо и отпечаток не заменить, а походку и голос снимают незаметно
- Определение биометрии в 152-ФЗ оставляет шесть пробелов
- Без цели установления личности снимок не биометрия

Биометрию определяют три признака, и только вместе

ч.1 ст.11 152-ФЗ: физиология, возможность установить личность и цель оператора

Privacy Advocates

Ч.1 СТ.11 152-ФЗ

Биометрические ПД

сведения, которые характеризуют **физиологические и биологические особенности** человека, на основании которых **можно установить** его личность и которые **используются оператором** для установления личности

1. **Физиология и биология**
   признак тела или поведения: лицо, голос, папиллярные узоры, вены, геном
2. **Позволяют установить личность**
   признак достаточно индивидуален, чтобы отличить человека от других
3. **Используются для установления**
   оператор применяет сведения именно для установления личности, отсюда строгий режим

ПРИМЕР	КАКИЕ ПРИЗНАКИ ЕСТЬ	РЕЖИМ
данные о здоровье	первый без третьего	специальные категории, ст.10
электронная подпись	второй без первого	общий режим, ст.6
городская видеозапись до опознания	первый и второй без третьего	общий режим, ст.6
фото в загранпаспорте	прямое указание ПП РФ от 04.03.2010 № 125	биометрия

Лицо и отпечаток не заменить, а походку и голос снимают незаметно

Физиологические и поведенческие характеристики несут разные риски

Privacy Advocates

Статические

Физиология, данная от рождения

- рисунок вен, папиллярные узоры пальцев и ладоней
- радужная оболочка и сетчатка глаза
- геномная информация (п.3 ст.1 242-ФЗ)
- фотография или видеоизображение лица
- **Риск:** при утечке признак не сменить, поэтому приоритет - защита хранилища и короткие сроки

vs

Динамические

Поведенческие характеристики

- голос, в котором физиология сочетается с манерой речи
- подпись с нажимом, направлением движений и штрихом
- клавиатурный почерк, походка, работа с сенсорным экраном
- **Риск:** признаки снимаются в фоне, страдает информированность согласия, приоритет - прозрачность сбора

Спорно: GDPR называет поведенческие признаки прямо, а ч.1 ст.11 говорит о физиологии и биологии, поэтому при установлении личности по поведению берут письменное согласие

Определение биометрии в 152-ФЗ оставляет шесть пробелов

Почему одни и те же сведения то признаются биометрией, то нет

Privacy Advocates

1 **Двойной критерий**

норма соединяет сведения, которые позволяют установить личность, и сведения, которые для этого используются, поэтому одно фото бывает и биометрией, и нет

2 **Нет понятия установления личности**

межотраслевого определения и процедуры нет, нормы есть лишь для отдельных правоотношений, момент установления не определен

3 **Чья обработка**

если эталон и сравнение остаются на устройстве пользователя, а оператор получает только результат, биометрию обрабатывает не оператор

4 **Аутентификация не названа**

норма говорит об установлении личности, но не о подтверждении того, что человек тот, за кого себя выдает

5 **Нет признака технических средств**

в отличие от GDPR не назван критерий специальных средств получения эталона и автоматического сравнения

6 **Точность не признак**

достоверность идентификации признаком не служит, а доли ошибочного допуска (FAR) и отказа (FRR) всегда больше нуля

Практика: режим задает процесс, а не файл: квалификацию пересматривают при каждом изменении назначения системы

Без цели установления личности снимок не биометрия

Третий признак: биометрическая аутентификация активна, а копии и архивы ею не являются

Privacy Advocates

ТРЕТИЙ ПРИЗНАК

Активное предъявление образа

Биометрическая аутентификация - проверка подлинности заявленного имени через предъявление своего биометрического образа и его преобразование по заранее определенному протоколу. Она почти всегда сцеплена с авторизацией, как дверной замок со сканером отпечатка

- пример: распознавание лиц водителей
- пример: биометрический учет рабочего времени

НЕ БИОМЕТРИЯ, ПИСЬМО МИНЦИФРЫ ОТ 28.08.2020 № ЛБ-С-074-24059

- ✕ скан паспорта для подтверждения действий конкретного лица без процедур идентификации
- ✕ ксерокопия документа, удостоверяющего личность
- ✕ фотография в личном деле работника
- ✕ подпись и почерк, в том числе для почерковедческой экспертизы
- ✕ рентгеновские и флюорографические снимки в медицинской карте
- ✕ видеосъемка в публичных местах и на охраняемой территории

Граница: снимки в медкарте остаются сведениями о здоровье по ст.10, а смена назначения системы переводит ту же съемку в биометрию без замены оборудования

Биометрию дают только добровольно и отдельным согласием

ч.4 ст.9 и ч.3 ст.11 152-ФЗ, чч.11-13 ст.3 572-ФЗ: что требуется и что запрещено

Privacy Advocates

Требуется

Письменное и свободное согласие

- письменная форма с реквизитами ч.4 ст.9 152-ФЗ, собственноручная или равнозначная электронная подпись
- с 01.09.2025 отдельный документ, а не пункт договора, анкеты или оферты (ч.1 ст.9)
- конкретному оператору и на одну цель: проход, учет времени и подтверждение операций оформляют раздельно
- работающий небиометрический маршрут без издержек для отказавшегося

vs

Запрещено

Понуждение и отказ в обслуживании

- требовать биометрию для договора, счета или абонемента, кроме случаев ч.2 ст.11 152-ФЗ
- обусловливать услугу, ее объем или количество товара прохождением биометрии (чч.11-13 ст.3 572-ФЗ)
- отказывать потребителю в договоре: ч.8 ст.14.8 КоАП, для юрлица 200-500 тыс. ₽
- отказывать в госуслуге из-за отказа от биометрии: ч.2.1 ст.5.63 КоАП с 30.05.2025

Практика: согласие через одноразовый код в личном кабинете банка признано ничтожным (88-14185/2025), а наказать работника за неотметку отпечатком после отзыва согласия суды не дали (88-24328/2022)

Ведомства 2020-2022: от любой фотографии к прямым указаниям

Позиции Минцифры, Роскомнадзора и Роструда об отнесении фото и отпечатков к биометрии

Privacy Advocates

10.02.2020

Роскомнадзор

№ 08АП-6782: рекомендации по биометрии детей, квалификация фото не привязана к формату

28.04.2020

Роскомнадзор

№ 08-24451: отпечатки вправе применять госорганы, у коммерческой организации оснований нет

17.07.2020

Минцифры

№ ОП-П24-070-19433: фото в СКУД - биометрия, биометрия учащихся для пропуска недопустима

28.08.2020

Минцифры

№ ЛБ-С-074-24059: копии паспорта, фото в личном деле, подпись, рентген не биометрия

19.11.2021

Роскомнадзор

№ 09-78548: разъяснения 2013 года, где биометрией были даже рост и вес, неактуальны

09.03.2022

Управление по СЗФО

№ 9627-12/78: фото не биометрично по сути, в нем нет термограммы, радужки и узоров

29.08.2022

Роскомнадзор

№ 08-78032: фото - биометрия при прямом указании НПА, например ПП РФ № 125, иначе ст.6

25.11.2022

Роструд

работодатель не вправе снимать отпечатки работников для пропускного режима

Позже: с августа 2025 года несоответствие ГОСТ уже не выводит фото из режима биометрии

Суды признавали биометрией фото на пропуске и вены ладони

Практика признания: от пропуска в спорткомплекс до узнаваемого лица в видеорепортаже

Privacy Advocates

ЧТО ПРИЗНАНО БИОМЕТРИЕЙ	СУДЕБНЫЙ АКТ
фотографии на пропусках	АС СЗО 21.11.2017 № Ф07-11732/2017, ВС РФ 05.03.2018 № 307-КГ18-101, дело № А42-342/2017
рисунок вен ладоней учащихся для оплаты питания и прохода	Лискинский районный суд 09.07.2018 № 12-35/2018
шаблон отпечатков в удостоверении личности моряка	Санкт-Петербургский горсуд 07.07.2020 № 33а-13473/2020
изображения с камеры в общей долевой собственности сторон	5 КСОЮ 28.09.2021 № 88-7100/2021
фото несовершеннолетних с ФИО в пропускной системе бизнес-центра	Зеленоградский районный суд 23.06.2022 № 12-0531/2022
отпечатки работника после отзыва согласия в организации с наркотическими препаратами	2 КСОЮ 01.11.2022 № 88-24328/2022
фото работника на сайте вакансий бывшего работодателя	2 КСОЮ 04.07.2023 № 88-13675/2023, компенсация 80 000 ₽ устояла
изображение узнаваемого лица в видеорепортаже	4 КСОЮ 26.09.2024 № 88-27709/2024, направлено на новое рассмотрение

Осторожно: перед ссылкой проверяют цепочку инстанций: фитнес-дело 12-1526/2019 отменено кассацией 16-937/2020 без оценки квалификации

Видео без цели опознания суды биометрией не считают

Практика непризнания: камеры, архивы до передачи, видеоурок и проверка живости

Privacy Advocates

Городские камеры

используются МВД для общественной безопасности: 2 КСОЮ 31.07.2020 № 88а-17020/2020, Мосгорсуд 30.01.2020 № 33а-707/2020

Частные камеры

не охватывают участок истцов и не позволяют достоверно идентифицировать лиц: ВС Республики Коми 04.02.2019 № 33-640/2019

Съемка на телефон

запись не позволяет идентифицировать субъекта: 4 КСОЮ 16.10.2020 № 16-894/2020

Камеры клиники

запись показана посетителю для поиска его телефона: 8 КСОЮ 19.12.2019 № 88-1005/2019

Камера в доме

не направлена на квартиру истца и служит охране владельца: Кировский районный суд Саратова 01.06.2021 № 2-2354/2021

Архив госоргана

записи до передачи в целях идентификации: Нижегородский облсуд 19.12.2018 № 33а-15421/2018

Спящий работник

изображение до передачи для установления личности: Кинешемский горсуд 27.05.2021 № 2-873/2021

Видеозапись урока

для дисциплины, без портретной съемки, удалена после занятия: Княжпогостский районный суд 04.02.2025 № 12-3/2025

Проверка живости

видеопроверка владельца профиля Авито не служит установлению личности: Рязанский облсуд 11.03.2026 № 33-342/2026

Отпечатки на объекте ТЭК

допустимы без согласия по антитеррористическим требованиям, ч.2 ст.11: 7 КСОЮ 01.08.2023 № 88-10266/2023

Прокуратура с ФСБ и Росгвардией нашла 170 фото детей

Дело старшего администратора ООО "Савелкинский проезд, д.4": фото учащихся в пропускной системе

Privacy Advocates

ПОЧЕМУ БИОМЕТРИЯ

Фото с ФИО для карт доступа

квалификация опиралась на определение ВС РФ от 05.03.2018 № 307-КГ18-101 и письмо Минцифры от 17.07.2020 № ОП-П24-070-19433. Письменных согласий родителей не было ни у управляющей компании, ни у центра обучения

- организацию оштрафовали на 30 000 ₽ отдельным постановлением (5-276/2022), замену предупреждением суд отклонил
- отстранение и лишение премии не освободили ответственного
- довод о компьютере прежней управляющей компании отклонен

1. **02.10.2021: хранение фото**

   на компьютерах администраторов бизнес-центра "Зеленоград" 170 фото учащихся компьютерного центра с фамилиями, именами и отчествами

2. **20.01.2022: проверка**

   прокуратура Зеленоградского округа по обращению гражданки с сотрудниками ФСБ и Росгвардии, файлы удалили через несколько минут после осмотра

3. **19.04.2022: штраф**

   мировой судья оштрафовал по ч.2 ст.13.11 КоАП старшего администратора, ответственного за ПД при оформлении карт доступа

4. **23.06.2022: решение устояло**

   Зеленоградский районный суд оставил штраф в силе, замену предупреждением и малозначительность отклонил

Роскомнадзор сузил биометрию в СКУД до контура 572-ФЗ

Позиции ведомств 2023-2026: фото, отпечатки, домофония и стройплощадки

Privacy Advocates

Биометрия

Признают биометрией

- **02.10.2023**, управления Роскомнадзора: отпечатки и фото пропуска при использовании в СКУД
- **28.12.2023**, Минцифры № П24-2-04-070-257558: домофония по лицу, если это аутентификация, подчиняется 572-ФЗ
- **13.03.2024**, управление по Астраханской области: сверка фото на пропуске с предъявителем
- **15.10.2025**, Минцифры № П24-16856-ОГ: отпечатки в СКУД, хотя 572-ФЗ на них не распространяется
- **06.03.2026**, Минцифры: на стройплощадках только ЕБС или аккредитованные системы и согласие

vs

Общий режим

Сужают режим или снимают согласие

- **23.04.2024**, Роскомнадзор № 08-128904: фото в СКУД - биометрия при подходе 572-ФЗ, в СКУД только данные ч.4 ст.3
- **01.08.2024**, управление по ЦФО № 62450-02-11/77: только при прямом указании НПА, иначе ст.6
- **06.03.2026**, Роскомнадзор № 08-166570: стройплощадки без согласия по ч.2 ст.11
- **14.08.2026**, день открытых дверей: лицо в СКУД вне ст.13 572-ФЗ не биометрия, вектор без установления личности тоже

Практически: позиция 2026 года устная и расходится с практикой по делу А42-342/2017: до письменного подтверждения сохраняйте письменное согласие и небиометрический проход

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OTV-003	Ландшафт юридической ответственности за ПД	30 Ответственность

15.3

ЕБС и 572-ФЗ

- Биометрическая система хранит не образ, а вектор
- ГОСТ раскладывает биометрическую систему на пять подсистем
- 572-ФЗ не применяется к ручному сравнению и ряду сфер
- Закон о ПД и закон о ЕБС называют личность по-разному

Биометрическая система хранит не образ, а вектор

Снятие, оцифровка и сравнение отличительной характеристики на примере отпечатка пальца

Privacy Advocates

1 **Снятие образа**

сканер или камера получают биометрический образец

2 **Извлечение признаков**

контроль качества, сегментация, выделение узоров и характерных точек

3 **Шаблон или вектор**

математическое преобразование в цифровую форму вида 10010011

4 **Сравнение**

проверка 1-к-1 с эталоном или поиск 1-к-n по базе

5 **Решение**

степень соответствия сравнивают с порогом и получают ответ да или нет

ПРАВОВОЙ СТАТУС

Вектор остается ПД

п.3 ст.2 572-ФЗ: ПД, полученные в результате математического преобразования биометрических ПД. Для него действуют цель, основание, сроки и права субъекта

- к векторам ЕБС не применяются ст.11 и меры защиты по ст.19 152-ФЗ (ч.5 ст.3 572-ФЗ), но общий режим ПД сохраняется
- векторное преобразование не является обезличиванием, а невосстановимость исходного образа вопрос о режиме не решает
- для идентификации через ЕБС порог соответствия не ниже 0,9999 задан приказом Минцифры от 17.04.2023 № 378

ГОСТ раскладывает биометрическую систему на пять подсистем

Компоненты биометрической системы общего вида по ГОСТ Р 54412-2019

Privacy Advocates

01

Сбор

сканер получает биометрическое предъявление, при низком качестве просит повторить

02

Обработка сигнала

контроль качества, сегментация, выделение признаков и создание шаблона

03

Хранение

база биометрических регистраций с контрольными шаблонами

04

Сравнение

сопоставление нового шаблона с базой и расчет результата

05

Решение

порог и правила: совпадение при верификации, кандидат при идентификации

ТРИ ПРОЦЕССА ПРОХОДЯТ ЧЕРЕЗ ПОДСИСТЕМЫ

биометрическая регистрация | биометрическая верификация | биометрическая идентификация

Для юриста: заведение базы образцов является юридическим решением: именно подсистема хранения и сравнения превращает снимки в биометрию

572-ФЗ не применяется к ручному сравнению и ряду сфер

Сфера действия 572-ФЗ и изъятия ст.1: по способу сравнения и по сфере деятельности

Privacy Advocates

152-ФЗ

Ручная обработка

сравнение ведет уполномоченное должностное лицо с реальным контролем над решением

- режим ч.1 ст.11 со всеми последствиями, включая письменное согласие
- законный выход из контура ЕБС при сохранении задачи опознания
- цена - ручной труд и зависимость от квалификации сотрудника

572-ФЗ

Автоматизированная обработка

сравнение изображения лица или записи голоса ведет информационная система

- идентификация только через ЕБС
- аутентификация через ЕБС, региональный сегмент или аккредитованную организацию по векторам
- поверх действует режим ст.11 152-ФЗ

ИЗЪЯТИЯ СТ.1 572-ФЗ

Закон не применяется в целях

- оперативно-разыскной, контрразведывательной и разведывательной деятельности
- обороны, безопасности государства, охраны правопорядка, внешней политики
- миграционного и регистрационного учета, обращения документов, удостоверяющих личность
- санитарно-эпидемиологического благополучия

Не путать: изъятия ст.1 572-ФЗ не совпадают с ч.2 ст.11 152-ФЗ: первые выводят из инфраструктурного закона, вторые освобождают от согласия

Закон о ПД и закон о ЕБС называют личность по-разному

Установление личности, идентификация и аутентификация: три термина вместо одного

Privacy Advocates

01

ч.1 ст.11 152-ФЗ

Установление личности

родовое понятие закона о ПД. Межотраслевого определения и универсальной процедуры нет, поэтому неясно, какие действия ему соответствуют

02

пп.6, 7 ст.2 572-ФЗ

Идентификация: кто это?

установление личности через установление сведений о лице и их проверку, сопоставление сведений с идентификатором

03

п.2 ст.2 572-ФЗ

Аутентификация: ты ли это?

проверка принадлежности лицу идентификаторов через сопоставление со сведениями проверяющего, после чего лицо считается установленным

Тонкость: 572-ФЗ разводит операции по предмету установления, а не по числу сравниваемых записей: аутентификация допускает и проверку 1-к-1, и поиск 1-к-n

С 2023 года биометрия переехала из 149-ФЗ в 572-ФЗ

Что изменилось для коммерческих биометрических систем (КБС) и банков

Privacy Advocates

АСПЕКТ	БЫЛО, 149-ФЗ	СТАЛО, 572-ФЗ
Сбор	банки по желанию гражданина собирают биометрию в ЕБС, собранное в КБС передается в ЕБС	то же, импорт лица и голоса из КБС и других систем в ЕБС до 30.09.2023
Хранение в КБС	хранить биометрию разрешено и в КБС, и в ЕБС	первичная биометрия только в ЕБС, в КБС векторы ЕБС и данные аутентификации до 10 суток, передавать векторы третьим лицам нельзя
Услуги КБС	идентификация и аутентификация по биометрии	идентификация только через ЕБС и ЕСИА, аутентификация только по векторам ЕБС, запретные случаи в ПП РФ № 815
Аккредитация КБС	по установленным требованиям с 01.03.2023	с 01.06.2023 с переходным периодом до 01.12.2023, защита на уровне ГИС с 01.01.2025
Согласия	сбор и обработка только с согласия	плюс согласие на передачу вектора в КБС, отказ от сбора через МФЦ, управление согласиями на Госуслугах с 01.01.2024

В ЕБС три уровня биометрии с разными лимитами

Уровень зависит от способа регистрации, по данным портала ЕБС для граждан

Privacy Advocates

приложение или импорт

Упрощенная

регистрация в приложении "Госуслуги Биометрия" по подтвержденной учетной записи Госуслуг: проезд, проход в офис, простые сервисы

- срок действия 2-3 года
- покупки до 2 500 ₽
- перечень услуг ограничен

приложение с NFC

Стандартная

нужны загранпаспорт с чипом, телефон с NFC и подтвержденная учетная запись: вход на Госуслуги, проход, проезд, сим-карта

- срок действия 2-3 года
- покупки до 5 000 ₽
- перечень услуг ограничен

очно в банке

Подтвержденная

доступ ко всем услугам по биометрии: замена паспорта, дистанционные банковские услуги, усиленная квалифицированная подпись

- срок действия 5 лет
- покупки до 5 000 ₽
- перечень услуг не ограничен

Новое: по изменениям порядка 2026 года гражданин вправе разместить в ЕБС оба вида биометрии или только один, поэтому у части пользователей есть лишь лицо или лишь голос

Какую биометрическую систему применять, зависит от объекта и задачи

Ст.13 572-ФЗ: где проход только через ЕБС, а где допустимы аккредитованные системы

Privacy Advocates

ОБЪЕКТ И ЗАДАЧА	ОПЕРАЦИЯ	ЧЕРЕЗ ЕБС	ЧЕРЕЗ КБС
Важные объекты ч.1 ст.13. ОПК, атомная и ядерная оружейная отрасли, химия, ТЭК, транспортная инфраструктура, субъекты КИИ, объекты с высоким риском теракта, режимные	идентификация и аутентификация	да	нет
Свои сотрудники, ч.3 ст.13. Госорганы и субъекты КИИ, которые сами аккредитованы, на своей территории	аутентификация	да	да
Остальные организации, ч.2 ст.13. Проход сотрудников и посетителей	аутентификация	да	по векторам
8 групп ПП РФ № 815. Экзамены, телемедицина, рецептурные препараты, госуслуги и ГИС, медосмотры и другие	аутентификация	да	нет

В работе: законопроект № 1131094-8 от 24.01.2026 открывает важным объектам собственные системы аккредитованного владельца для сотрудников и посетителей, но пока не принят

С ЕБС работают по двум моделям: транзакционной и векторной

ЕБС - государственная система, оператор АО "Центр Биометрических Технологий" (ПП РФ № 834)

Privacy Advocates

ЕБС хранит изображение лица и запись голоса. Идентификация через ЕСИА и ЕБС приравнивается к предъявлению паспорта, кроме случаев, когда закон требует оригинал документа

Транзакционная

Каждое сравнение идет в ЕБС

- организация запрашивает ЕБС и ЕСИА при каждом обращении клиента
- доступны идентификация и аутентификация
- эталоны остаются в ЕБС, организация получает только результат
- плата за каждое успешное сравнение

vs

Векторная

Сравнение в аккредитованной системе

- векторы ЕБС передаются в КБС аккредитованной организации
- доступна только аутентификация
- нужны шесть условий ст.16 572-ФЗ, включая аккредитацию
- плата за передачу векторов

Транзакционная модель: ЕБС отвечает, кто это и тот ли это

Идентификация для создания профиля и аутентификация владельца профиля

Privacy Advocates

ИДЕНТИФИКАЦИЯ: УСТАНОВИТЬ ЛИЧНОСТЬ И СОЗДАТЬ ПРОФИЛЬ

1

Запрос клиента

человек хочет стать клиентом

2

Запрос сведений

организация запрашивает ЕБС и ЕСИА о гражданине

3

Ответ системы

это Иванов И.И., паспорт и другие данные

4

Обслуживание

организация создает профиль клиента

АУТЕНТИФИКАЦИЯ: ПОДТВЕРДИТЬ, ЧТО ОБРАТИЛСЯ ВЛАДЕЛЕЦ ПРОФИЛЯ

1

Запрос услуги

клиент хочет войти в личный кабинет

2

Сравнение

фото уходит в ЕБС: это id 42 (1-к-1) или кто это (1-к-n)

3

Ответ ЕБС

да, это id 42, либо это id 63

4

Оказание услуги

допуск в личный кабинет

Не забыть: перед аутентификацией клиентскую базу с идентификаторами выгружают в ЕСИА, это самостоятельная обработка ПД

Векторная модель требует шести условий одновременно

Аутентификация в КБС аккредитованной организации: согласие через ЕСИА, векторы из ЕБС

Privacy Advocates

Условия ч.3 ст.16 572-ФЗ соединены: без любого из них векторная аутентификация недоступна

1. меры защиты по ч.4 ст.19 152-ФЗ
2. СКЗИ против угроз, определенных уполномоченными органами
3. требования к сбору биометрических ПД
4. требования 572-ФЗ и законодательства о безопасности КИИ
5. согласие физлица, им управляют через ЕСИА
6. аккредитация организации по ст.17 572-ФЗ

без аккредитации, путь 1

Прекратить старый режим

сервисы с биометрией вне правил 572-ФЗ ведут к ответственности по ст.13.11.3 КоАП

путь 2

Работать через ЕБС

пользоваться услугами ГИС ЕБС по идентификации и аутентификации

путь 3

Договор с аккредитованной

своя аккредитация не нужна, если у организации нет собственной биометрической системы

Фильтр участника: организация вне перечней экстремистов и террористов, руководитель без судимости, в ЕГРЮЛ нет записи о недостоверности, при векторной модели проверяет аккредитованная организация

Для аккредитации нужно не меньше 500 млн ₽ собственных средств

Ч.2 ст.17 572-ФЗ, ПП РФ № 810 и перечень обязательных требований Минцифры от 28.04.2026

Privacy Advocates

500 млн ₽

собственные средства

капитал организации

100 млн ₽

финобеспечение

ответственности за убытки

49%

иностранное участие

предел доли в капитале

3 года

без отзыва

аккредитации досрочно

- базы данных только в России
- подключение к ГосСОПКА
- лицензия ФСБ, если криптография не только для своих нужд
- аппаратные шифровальные средства в собственности
- два сотрудника с высшим ИТ-образованием
- согласие на раскрытие налоговой тайны
- нет записи о недостоверности в ЕГРЮЛ

ЕДИНОЛИЧНЫЙ ИСПОЛНИТЕЛЬНЫЙ ОРГАН

- гражданство России, деловая репутация
- нет в перечнях экстремистов и террористов
- нет неснятой или непогашенной судимости
- 5 лет без наказаний за разглашение тайн
- 3 года не руководил организацией с отозванной аккредитацией

Обращение к ЕБС платно для всех, кроме госорганов

Приказ Минцифры от 31.03.2023 № 334: тарифы 30 и 10 ₽ с коэффициентами 2, 1,5 и 1 по объему за день

Privacy Advocates

КАТЕГОРИЯ, ПЛАТА ЗА УСПЕШНОЕ СРАВНЕНИЕ С НДС	КОЭФ.	1-500 В ДЕНЬ	501-1000	ОТ 1001
Идентификация, все категории пользователей	1	60 ₽	45 ₽	30 ₽
Аутентификация: проход на территорию, безналичные расчеты в торговле и услугах, налоги и сборы	0,14	2,80 ₽	2,10 ₽	1,40 ₽
Аутентификация пассажиров поездов дальнего следования и пригородных	0,5	10 ₽	7,50 ₽	5 ₽
Аутентификация: возраст при продаже алкоголя и табака, рецептурные лекарства, иные категории	1	20 ₽	15 ₽	10 ₽
Совместные мероприятия по популяризации биометрии по соглашению с оператором ЕБС	0	0	0	0

Есть месячные пакеты: идентификация 285 000 ₽ за 10 тыс., 810 000 ₽ за 30 тыс. и 2 550 000 ₽ за 100 тыс. успешных сравнений, аутентификация с коэффициентом 1 - 95 000, 270 000 и 850 000 ₽

Учесть: методика действует до 01.06.2029, госорганы и Банк России от платы освобождены, а по расчету к законопроекту 2026 года проход через ЕБС стоит 2,8 ₽ при годовой плате 30 ₽ за вектор

К 2027 году контур 572-ФЗ пересоберут еще раз

Вступление в силу 572-ФЗ и ключевые даты переходного периода

Privacy Advocates

2022-2024: ЗАПУСК

29.12.2022

Принят 572-ФЗ

основная часть действует со дня опубликования

01.06.2023

Ст.13-18

запреты ст.15, проход, аккредитация, векторная модель, надзор

30.09.2023

Закрыт импорт

истекло окно передачи ранее собранной биометрии в ЕБС

01.01.2024

Госуслуги

просмотр и отзыв всех согласий в режиме одного окна

01.09.2024

Виды решает Правительство

ПП РФ № 408: лицо и голос до 01.09.2027

2025-2029: ПЕРЕСТРОЙКА

01.01.2025

Защита КБС

требования к системам на уровне ГИС

2026

В работе

законопроект о ст.13, по СМИ МФО ждут идентификации по лицу

01.01.2027

Регионы и подпись

сегменты на векторах, конец переходной ПЭП

01.09.2027

Перечень видов

истекает ПП РФ № 408, виды определят заново

01.06.2029

Тарифы

истекает методика платы за обращения

15.4

СКУД, сценарии и встраивание в продукты

- Идентификацию по лицу и голосу ведут только через ЕБС
- Аутентификация по лицу возможна в ЕБС или по ее векторам
- Фото в СКУД: чем меньше автоматики, тем меньше риска
- Режим задают установление личности и биораспознавание

Идентификацию по лицу и голосу ведут только через ЕБС

Биометрическая идентификация: установление личности через установление сведений о лице

Privacy Advocates

ДЕФИНИЦИИ

Идентификация, п.7 ст.2 572-ФЗ

совокупность мероприятий по установлению сведений о лице и их проверке и сопоставлению этих сведений с идентификатором

- идентификатор - уникальное обозначение сведений о лице для его определения (п.6 ст.2 572-ФЗ)
- по ГОСТ ISO/IEC 2382-37-2016 - поиск по базе регистраций и возврат идентификатора шаблона одного индивида

Алгоритм

получение сведений о лице из ЕСИА и ЕБС по транзакционной модели

Запрет своей системы

ст.15 572-ФЗ запрещает организациям обрабатывать, собирать и хранить биометрию для идентификации, кроме сбора для размещения в ЕБС

Нормативный порог

степень соответствия не ниже 0,9999 задана приказом Минцифры № 378, а не настройкой пользователя

Сила результата

идентификация через ЕБС и ЕСИА приравнивается к предъявлению паспорта (ст.11 572-ФЗ)

Первичный сбор

исходные лицо и голос принимают банки, МФЦ и уполномоченные организации либо сам гражданин через приложение

Аутентификация по лицу возможна в ЕБС или по ее векторам

Биометрическая аутентификация: установление личности путем установления самого лица

Privacy Advocates

Если технический процесс, реализуемый в сервисе домофонии, соответствует определению аутентификации, то организациям, предоставляющим такой сервис, необходимо соблюдать требования Федерального закона № 572-ФЗ

Минцифры России, информационное письмо от 28.12.2023 № П24-2-04-070-257558

АУТЕНТИФИКАЦИЯ, П.2 СТ.2 572-ФЗ

1. проверка принадлежности лицу идентификаторов через сопоставление со сведениями проверяющего
2. поиск 1-к-n или проверка 1-к-1 в ЕСИА и ЕБС либо в КБС по векторам

ВЕРИФИКАЦИЯ ПО ГОСТ

подтверждение биометрического заявления при сравнении, ГОСТ ISO/IEC 2382-37-2016 п.37.08.03

Вывод: домофония и проход по лицу - это аутентификация: только через ЕБС или по ее векторам в аккредитованной системе, собственная база шаблонов лица запрещена ст.15 572-ФЗ

Фото в СКУД: чем меньше автоматики, тем меньше риска

Четыре сценария использования фотографии для управления физическим доступом

Биометрия в СКУД
скачать

Privacy Advocates

01

общая категория

Небиометрическая обработка

- фото и сведения о посетителе на пропуске
- уполномоченное лицо сличает фото с лицом и решает о пропуске
- **Легализация:** ч.1 ст.6 152-ФЗ, вне ЕБС

02

общая или биометрия

Сличение на мониторе

- фото в СКУД, посетитель прикладывает id-карту
- СКУД показывает фото оператору, тот сравнивает и решает
- **Легализация:** ч.1 ст.6 или ст.11 152-ФЗ, вне ЕБС

03

биометрия

Биометрическая аутентификация

- в СКУД вектор и id-карта
- сенсор снимает лицо, СКУД сравнивает с шаблоном карты и решает без человека
- **Легализация:** только по векторам ЕБС (ч.1 ст.15, чч.1, 3 ст.16 572-ФЗ)

04

биометрия

Поиск по базе и решение

- шаблоны всех посетителей в СКУД
- сенсор снимает лицо, СКУД ищет совпадение в своей базе и сама решает
- **Легализация:** свои шаблоны запрещены ст.15 572-ФЗ, только ЕБС или ее векторы

Спорно: Роскомнадзор 14.08.2026 устно относит фото в СКУД к биометрии только в контуре ст.13 572-ФЗ, а суды по делу А42-342/2017 считали биометрией и ручную сверку

Режим задают установление личности и биораспознавание

Шесть клеток: как устанавливают личность и есть ли биометрическое распознавание

Сценарии биометрии
скачать

Privacy Advocates

Установление личности	Без биометрического распознавания сравнения нет или его ведет человек	С биометрическим распознаванием автоматическое сравнение системой
Личность не устанавливается	**1** **ч.1 ст.6 152-ФЗ** охрана и контроль производства по видео, фотофиксация полок, метки на форме и инвентаре	**2** **ч.1 ст.6, самая уязвимая клетка** подсчет уникальных посетителей, контроль СИЗ, угрозы в толпе, расшифровка ВКС по голосам, усталость водителя
Небиометрическое установление личности	**3** **ч.1 ст.6 152-ФЗ** охранник сличает фото на пропуске, видеоконтроль дисциплины, ручная проверка живости владельца профиля	**4** **ч.1 ст.6, клетка спорная** автосличение селфи с паспортом, проверка живости и возраста, вход по FaceID на устройстве пользователя
Биометрическое установление личности	**5** **ст.11 152-ФЗ без 572-ФЗ** должностное лицо ищет злоумышленника по записям камер и имеющимся образцам	**6** **ст.11 и 572-ФЗ** аутентификация в колл-центре, оплата проезда по лицу, каршеринг через ЕБС, отпечаток в СКУД только по ст.11

⚠ **Ловушка:** сверка с базой мошенников и сбор биометрии неклиентов по лицу и голосу образуют запрещенную собственную систему ст.15 572-ФЗ, а по иным модальностям нет ни основания, ни согласия

Встраивание биометрии упирается в семь ограничений

Что учесть до проектирования ИТ- или ИИ-продукта с биометрией

Privacy Advocates

1 Закрытый перечень ЕБС

с 01.09.2024 виды определяет Правительство: лицо и голос (ПП РФ № 408 до 01.09.2027), геном в ЕБС запрещен, отпечатки, вены и радужка живут по ст.11

2 Только Россия

идентификация и аутентификация с трансграничной передачей запрещены (ч.21 ст.3 572-ФЗ), зарубежные облака распознавания вроде AWS Rekognition и Azure Face закрыты

3 Своя идентификация запрещена

по лицу и голосу собственная идентификация запрещена ст.15 572-ФЗ, аутентификация только по векторам ЕБС, с аккредитацией, СКЗИ и лицензией ФСБ

4 Особый режим согласия

отдельное письменное согласие конкретному оператору, отзыв в любой момент, отказ не повод отказать в услуге или ухудшить ее условия

5 Несовершеннолетние

Минцифры сочло биометрию учащихся в СКУД школ недопустимой, согласие законного представителя не заменяет согласия самого субъекта

6 Пределы точности

FAR и FRR всегда больше нуля, качество падает с возрастом, после травм, при плохой съемке, поэтому спорные срабатывания закладывают в продукт

7 Сырой биометрии нет

из ЕБС выходят вектор и степень соответствия, а не изображение, это ограничивает дообучение своих моделей, данные аутентификации хранят до 10 суток

Биометрический продукт несет семь ключевых рисков

От необратимой утечки до проверок с участием ФСБ и Росгвардии

Privacy Advocates

Необратимость утечки

биометрию нельзя перевыпустить как пароль: скомпрометированный шаблон остается уязвимостью пожизненно и во всех системах

Штрафы и уголовный риск

утечка биометрии 15-20 млн ₽, повторная 1-3% выручки, но не менее 25 млн ₽, нарушения с ЕБС до 2 млн ₽, ч.2 ст.272.1 УК до 5 лет

Смещение моделей

по данным NIST FRVT точность распознавания различается по демографическим группам, это повод для жалоб и проверок

Атаки на предъявление

маски, фото, видео, deepfake, синтез голоса и подмена кадров в канале требуют многослойной проверки живости

Function creep

СКУД начинают применять для оценки производительности без легализации, вопреки целевому характеру и минимизации (ст.5 152-ФЗ)

Репутация

распознавание лиц в метро и биометрия в школах показали, что любая биометрическая инициатива под медийным микроскопом

Проверки

прокурорские проверки с ФСБ и Росгвардией ведут к штрафам и удалению данных, как в деле Савелкинского проезда 2022 года

Риски снижают архитектура и дисциплина процессов

Рекомендации продуктовым командам

Privacy Advocates

Архитектура и данные

- не применять биометрию, если цель достигается картой, PIN или OTP: она не выбор по умолчанию
- обрабатывать на устройстве: образ не покидает смартфон или терминал, оператор получает только да или нет
- хранить шаблоны вместо исходников, шифровать, ротировать ключи, уничтожать средством с автоудалением
- выбрать путь в ЕБС: своя аккредитация или договор с аккредитованной организацией из перечня ebs.ru
- сертифицированные алгоритмы и проверка живости, регулярные тесты FAR, FRR и устойчивости к deepfake

Процессы и комплаенс

- до запуска оценить необходимость, пропорциональность, альтернативы и вред для субъектов
- брать отдельное письменное согласие на каждую цель и держать небиометрическую альтернативу без ухудшения условий
- вести журналы согласий и отзывов, уведомлять Роскомнадзор об утечке за 24 и 72 часа
- фиксировать цели и оценивать каждое новое применение биометрии, чтобы избежать function creep
- уничтожать биометрию уволенных и отозвавших согласие по событию, а не при инвентаризации

Прозрачность: объясняйте пользователям простым языком, какие признаки снимаются, зачем, где хранятся и как их удалить, особенно в поведенческой биометрии

15.5

Видеонаблюдение

- Камеру ставят под конкретную цель и проверяют, что попадает в кадр
- Пиктограмма камеры еще не информирует о наблюдении
- Срок хранения записей задает цель, а не объем регистратора
- Запись с камеры весомее, если ее сняли и выдали по правилам

Камеру ставят под конкретную цель и проверяют, что попадает в кадр

Основание зависит от объекта и цели, а зону обзора ограничивают ожидания людей и реальный сектор камеры

Privacy Advocates

СИТУАЦИЯ	ОСНОВАНИЕ	ПРЕДЕЛ
Норма требует камер	п.2 ч.1 ст.6: массовое пребывание (ПП № 272), все гостиницы (ПП № 447), медицина 3-й и выше категорий (ПП № 8)	оснащение закрыто, доступ и выдача нет
Посетители	законный интерес п.7 ч.1 ст.6 при конкретной задаче и учете ожиданий	проверка мягкого способа, спорно
Работники	охрана входов или контроль рабочих мест по п.1 ст.86 ТК	ст.214.2 ТК только для безопасности работ
Гражданин и МКД	личные нужды (ч.2 ст.1) или решение собрания (88-100/2019)	обзор на соседа выводит из изъятия

ГДЕ КАМЕРЫ НЕТ

- по экспертному подходу примерочные, раздевалки, уборные, смотровая кабинета врача и точки, раскрывающие здоровье или убеждения
- суд исключил комнату отдыха и приема пищи, хотя приказ не оспорен (88-14171/2023)

КАДР, А НЕ ПЛАН

- в спорах соседей обзор не шире взгляда обычного наблюдателя обработкой ПД не признан (33-640/2019, 88-235/2021)
- сектор доказывают экспертизой (88-6070/2023) и выгрузкой кадра (2-177/2022)
- звук, по экспертному подходу, обосновывают отдельно

Пиктограмма камеры еще не информирует о наблюдении

Момент, содержание и форма извещения, требование 427-ФЗ с 01.09.2026 и четыре слоя документов режима

Privacy Advocates

427-ФЗ, Ч.3 СТ.10, С 01.09.2026

Сведения до входа на объект

при охранной услуге с видеонаблюдением людей информируют до входа, на видном днем и ночью месте, с условиями режима и правилами допуска, а обязанность оператора по ПД остается

ПАРАМЕТР	РАБОТНИК	ПОСЕТИТЕЛЬ
Момент	до начала наблюдения, новичок при приеме на работу	до входа в зону
Содержание	факт, цель и зоны видимости камер	факт и цель, при охране условия режима
Форма	локальный акт под роспись, трудовой договор, таблички	табличка и политика обработки

1

Решение

приказ с датой начала, целью и ответственным

2

Локальный акт

цели, точки, состав, доступ, срок, передача и сбой

3

Информирование

лист ознакомления, таблички, раздел политики

4

Обвязка

перечни ПД и ИСПД, поручение охране

Практика: при открытом наблюдении суды принимали приказ, схему камер и лист ознакомления (33-653/2019) или приказ, положение и личное уведомление работника (33-20507/2016), а негласное наблюдение документами не исцеляется

Срок хранения записей задает цель, а не объем регистратора

Ориентиры глубины из норм и рекомендуемый порядок работы с фрагментами, массивом и доступом к записям

Privacy Advocates

30 суток

гостиницы

архив непрерывного наблюдения, ПП № 447

1 месяц

медицина и наука

ПП № 8 от 3-й категории, ПП № 1421 для 1-й и 2-й

6 месяцев

предел уничтожения

блокированного массива, если закон не задал иное (ч.6 ст.21)

1. **Закрепить срок заранее**
   по цели в локальном акте, со сверкой с глубиной регистратора
2. **Выгрузить фрагмент**
   при инциденте до перезаписи, с отметкой момента выгрузки
3. **Дать фрагменту свой срок**
   до конца разбирательства, иначе копии живут годами в почте
4. **Закрыть неизвлекаемый массив**
   блокировать и уничтожить целиком

ДОСТУП В ДВА СЛОЯ

- пост видит живое изображение, но не выгружает архив
- администратор обслуживает систему без доступа к записям
- каждое обращение к архиву журналируется
- доступ, повлекший копирование, блокирование, модификацию или уничтожение, грозит ст.272, 272.1 УК

Запись с камеры весомее, если ее сняли и выдали по правилам

Когда запись примут в суде, кто вправе ее смотреть, как выдать органам и субъекту и чем рискует оператор

Privacy Advocates

В СУДЕБНОМ СПОРЕ

- аудио и видео названы доказательствами (ч.1 ст.55 ГПК, ст.26.7 КоАП), допустимость оценивают в каждом производстве
- просмотр защищен, когда подтвердил уже выявленный и не оспоренный факт (33-50244/2018), а довод о п.6 ст.86 ТК в 33-8775/2018 отклонен

ЭКСПЕРТНЫЙ ПОДХОД

- поиск повода по архиву и решение на одной выгрузке защищаются хуже
- запись с нарушением порядка теряет вес и может дать требование о моральном вреде (ст.24 152-ФЗ, ст.237 ТК)

ВЫДАЧА ОРГАНУ ПО П.4 Ч.1 СТ.13 ЗАКОНА О ПОЛИЦИИ

1. **Основание и полномочие**
   норма запроса и полномочие запрашивающего
2. **Форма запроса**
   запрос оформлен так, как требует норма
3. **Объем**
   фрагмент по предмету запроса, а не архив за период
4. **Фиксация**
   кому, когда и что передано

Доступ: по ст.14 субъекту сообщают сведения о наблюдении, отказ мотивируют нормой (ч.8 ст.14), хотя обязанности знакомить работника с записью прохода суд не нашел (88-19944/2023). При передаче вовне, например в СМИ, посторонних маскируют

Видео становится биометрией, когда по нему устанавливают личность

Три состояния изображения по ч.1 ст.11 152-ФЗ, распознавание, поиск по архиву и передача записи полиции

Privacy Advocates

1

Поток

лица в кадре без сопоставления, обычные ПД с основанием наблюдения

2

Архив

запись получает время и связи, нужны срок, состав и основание удержания

3

Установление личности

по кадру включает ст.11, а выемка и сравнение без него режим не включают (2а-577/19)

СОБЫТИЕ	КАК КВАЛИФИЦИРУЮТ	ЧТО ДЕЛАТЬ
Включили распознавание	по экспертному подходу меняет режим всего массива, если массив служит установлению личности	дату функции фиксируют, основание, меры и уведомление пересматривают
Ищут виновного по архиву	по экспертному подходу это ст.11, Роскомнадзор устно (22.10.2025, 14.08.2026) видит биометрию лишь по закону о биометрии	согласие на цель расследования рекомендуют брать заранее
Передали запись полиции	полиция вправе устанавливать личность без согласия (ч.2 ст.11, ч.1 ст.13 закона о полиции, ВС РФ 15.05.2025)	по экспертной оценке признака у оператора нет, основание и срок записи на нем

Пример: 7 КСОЮ 24.07.2020 вернул на новое рассмотрение жалобу школы на штраф 25 тыс. ₽ по ч.5 ст.13.11 КоАП, не оценен довод о согласии родителей, законность не решалась (16-2185/2020)

Режим биометрии задает цель, а закон выбирают по виду признака

Ключевые выводы раздела

Privacy Advocates

01

Режим включает цель

три признака ст.11 работают вместе: без цели установления личности снимок остается обычными ПД, формат ГОСТ ничего не решает

02

Лицо и голос в контуре ЕБС

идентификация только через ЕБС, аутентификация только по ее векторам с аккредитацией, остальные модальности живут по ст.11

03

Согласие отдельное и свободное

с 01.09.2025 отдельный документ, отказ без последствий, а отказ в договоре наказуем по ч.8 ст.14.8 КоАП

04

СКУД остается зоной спора

Роскомнадзор в 2026 году сузил биометрию до ст.13 572-ФЗ, суды и Минцифры шире: держите согласие и небиометрический проход

05

2027 - точка пересборки

региональные сегменты на векторах, конец переходной ПЭП, а с 01.09.2027 перечень видов биометрии определят заново

06

Антифрод без чужой биометрии

базу мошенников по лицу и голосу вести нельзя, строят ее на небиометрических признаках

16

Генетические данные

Регулирование оборота и трансграничной передачи в РФ

16.1 Понятие и режим

16.2 ТПД генетических данных

16.3 Риски и ответственность

Раздел на сайте
privacy-advocates.ru/pd/gen

16.1

Понятие и режим

- Генетические данные

Генетические данные

Что это и под какое регулирование подпадает

Privacy Advocates

ОПРЕДЕЛЕНИЕ

Генетические данные человека - сведения о последовательности нуклеотидов в полимерах нуклеиновых кислот и их химических модификациях, полученные молекулярно-генетическими методами исследования биологического материала человека.

КВАЛИФИКАЦИЯ И РЕЖИМ

Признак	**Геномная информация** 242-ФЗ	**Генетические данные человека** 86-ФЗ · ред. 43-ФЗ
Прямая квалификация	Биометрические ПД - прямо названо в дефиниции	Не квалифицируется в терминах 152-ФЗ
Объем	Узкий: кодированная информация об определенных фрагментах ДНК (профиль идентификации)	Широкий: вся последовательность нуклеотидов + их химические модификации из МГИ
Целевая функция	Идентификация лица или неопознанного трупа	Получение содержательных сведений из исследования биоматериала
Тяготеет к	Биометрия - ст. 11 (установление личности)	Спецкатегория - ст. 10 (здоровье) и/или биометрия
Режим	152-ФЗ ст. 11 + спецрежим 242-ФЗ (ФБДГИ)	Секторальный 86-ФЗ (трансгран. передача); статус ПД - по общим правилам

16.2

ТПД генетических данных

- Трансграничная передача
- Кому запрещена передача
- Состав Межведомственной комиссии
- Генетику за рубеж передают по маршруту из пяти шагов

Трансграничная передача

Постановление № 750

Privacy Advocates

Межведомственная комиссия - решает вопросы передачи генетических данных за пределы РФ

Разрешительный (общий)

- Передача за пределы РФ по решению Комиссии (п.2, форма решения - Приложение № 1).
- Плата за выдачу разрешения не взимается.
- Без разрешения Комиссии - международное сотрудничество, а медпомощь и разработка ЛП для пациента только у лицензиатов.

Разрешительный (заявление)

- Популяционные / иммунологические исследования в исключительных случаях.
- Форма - Приложение № 3. Комиссия рассматривает 15 раб. дней. Основания для отказа прямо перечислены (п.12).

Уведомительный

- Публикация научных результатов только со сводными показателями, не содержащими данных конкретных лиц.
- Уведомление не позднее чем за 20 раб. дней; у Комиссии 15 раб. дней на решение о доработке публикации.

Кому запрещена передача популяционных данных

Ч.1 ст.13.2 86-ФЗ: иностранные лица и их представители, исключения только через Комиссию

Privacy Advocates

Получатель	На территории РФ	За пределами РФ
Российское лицо	вне запрета	запрещено
Иностранное лицо, его филиалы и представители	запрещено	запрещено
Иностранное государство	запрещено	запрещено

Российское лицо: сбор и хранение на территории РФ - вне разрешительного порядка передачи за пределы РФ. "Российское лицо" определяется от обратного - за вычетом лиц, указанных в ст. 13.2 86-ФЗ.

Представители

АНТИОБХОД

"Представители" в запрете: иностранное юрлицо не получит данные через агента или представителя в РФ.

Передача квалифицируется **по существу** (в чьих интересах и под чьим контролем данные), а не по форме (где точка получения).

Представитель приравнен к иностранному доверителю - запрет действует и внутри РФ.

Состав Межведомственной комиссии

Орган, принимающий решения о трансграничной передаче генетических данных

Privacy Advocates

Правительство и министерства

- Аппарат Правительства РФ
- Минздрав России
- Минобрнауки России
- МИД России

Службы и надзор

- ФМБА России
- Роспотребнадзор
- ФСБ России
- ФСТЭК России

Наука и образование

- РАН
- МГУ им. М.В. Ломоносова
- СПбГУ
- НИЦ "Курчатовский институт"

А также подведомственные указанным органам организации. Председатель Комиссии - Заместитель Председателя Правительства РФ, курирующий здравоохранение; кворум - 2/3 членов, решения - простым большинством участвующих, работу Комиссии обеспечивает ФМБА России.

Генетику за рубеж передают по маршруту из пяти шагов

ПП № 750 от 15.06.2026 и ст.13.1-13.2 86-ФЗ: сначала получатель и цель, потом комиссия

Privacy Advocates

1

Получатель

данные популяционных исследований иностранцам не передают даже в России, кроме решения комиссии и публикации сводных показателей с уведомлением

2

Свободный перечень

медпомощь и препараты для конкретного пациента при лицензии, международное сотрудничество

3

Уведомление

публикация популяционных исследований только со сводными показателями, уведомление комиссии за 20 рабочих дней

4

Разрешение

в прочих случаях нужно решение комиссии, а заявление и 15 рабочих дней с продлением Правила задают только для популяционных данных

5

152-ФЗ

параллельно требования о ПД, а популяционные данные передают обезличенными

Ошибка: требование журнала депонировать первичные данные в открытую базу под уведомительный порядок не подпадает: он рассчитан на сводные показатели. Сроки комиссии закладывают в график до договора с партнером

16.3

Риски и ответственность

- Основные риски: квалификация данных
- Зоны повышенного риска
- Биоматериалы и генетические данные в КИ
- Иные риски и ответственность

Основные риски: квалификация данных

Где проходит граница "генетических данных"

Privacy Advocates

Проблема

ПП РФ № 750 не разграничивает **"сырые" генетические данные** и **медицинское заключение** (вывод о наличии / отсутствии мутации).

Широкие формулировки - "генетический статус", "аннотирование генетических данных", "молекулярно-генетический анализ" - распространяют регулирование и на первичные файлы секвенирования, и на производные результаты анализа.

Консервативный подход

РЕКОМЕНДАЦИЯ

Любую информацию, позволяющую сделать вывод о наличии, отсутствии или вероятности генетического варианта (мутации), безопаснее рассматривать как **генетические данные человека** для целей данного регулирования.

Зоны повышенного риска

Где трансграничная передача наиболее проблематична

Privacy Advocates

Международные клинические исследования

- С высокой вероятностью не подпадают под критерий "международного сотрудничества".
- Клинические группы пациентов могут квалифицироваться как объекты популяционных исследований - исключение для "конкретных пациентов" не применяется.

Спонсируемые диагностические программы

- Передача в зарубежную референс-лабораторию или централизованную базу штаб-квартиры невозможна (вне "международного сотрудничества") без лицензии на медицинскую деятельность (п. 3 Правил).
- Риск квалификации как популяционного исследования.

Научные публикации и депонирование

- Публикация результатов популяционных исследований требует предварительного уведомления.
- Требование ряда международных издательств депонировать первичные обезличенные данные в глобальные открытые базы практически невыполнимо.

Биоматериалы и генетические данные в КИ

Письмо Минздрава России от 21.05.2026 № 25-2/6504

Privacy Advocates

Разграничение режимов

Клинические исследования - по **61-ФЗ** и Правилам GCP ЕАЭС (Решение Совета ЕЭК № 79).

Вывоз биоматериалов при КИ - по постановлению Правительства РФ от 14.03.2022 № 363. Протокол КИ обязан указывать наименования и адреса лабораторий (п. 6.1.7 Правил).

Позиция Минздрава

ВЫВОД ИЗ ПИСЬМА

Прямого ответа о применимости 43-ФЗ к клиническим исследованиям регулятор не дал, сославшись на готовившийся акт ФМБА - теперь это ПП № 750. Статус генетических данных в международных КИ остается **зоной неопределенности**.

Иные риски и ответственность

О чем нельзя забывать

Privacy Advocates



Локализация баз данных ПД граждан РФ

Полный цикл первичной обработки (запись, систематизация, накопление, хранение, уточнение, извлечение) данных граждан РФ - включая сведения о мутациях, привязанные к ФИО или ID пациента - **только на серверах в РФ**.



Оборотные штрафы за утечки

Штрафы за инциденты со специальными категориями ПД **(утечка ПД)** не имеют градации по объему - назначаются за сам факт.



Уголовная ответственность

до 5 лет лишения свободы

Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации со специальными категориями ПД - ч.2 ст. 272.1 УК РФ.

КЛЮЧЕВЫЕ ВЫВОДЫ

- Любую информацию о наличии или вероятности генетического варианта ***безопаснее*** квалифицировать как генетические данные человека.
- Трансграничная передача - через Межведомственную комиссию (разрешительный либо уведомительный порядок), без ее разрешения только международное сотрудничество, медпомощь и разработка препаратов для конкретного пациента. Регулирование действует с 01.09.2026.
- Локализация данных, оборотные штрафы за утечки и уголовная ответственность (до 5 лет) - зоны особого внимания.

17

Права субъектов и обращения

Права субъекта, обращения, сроки ответа и особые субъекты

17.1 Права и лестница сроков

17.2 Прием обращения и идентификация заявителя

17.3 Ответ, отказ и надзорный след

17.4 Особые субъекты

Раздел на сайте
privacy-advocates.ru/pd/sub

17.1

Права и лестница сроков

- Права субъекта закон описывает через обязанности оператора
- По GDPR у человека больше прав, чем по 152-ФЗ
- Из семи сроков исполнения требований продлевают только десятидневный
- Ст.16 об автоматизированных решениях требует трех условий сразу

Права субъекта закон описывает через обязанности оператора

Сводного каталога нет: право собирают из ст.9, 14-16, 20, 21 и 10.1 152-ФЗ, ст.10.3 149-ФЗ и ТК

Privacy Advocates

Информирование и доступ

по запросу (ст.14, 20) и до начала обработки ПД, полученных не от субъекта (ч.3 ст.18)

Уточнение, блокирование, уничтожение

неполных, неточных, устаревших, незаконно полученных или ненужных ПД (ч.1 ст.14, ст.21)

Прекращение обработки

отзыв согласия (ч.2 ст.9, ч.5 ст.21) и требование прекратить обработку (ч.5.1 ст.21), кроме оснований пп.2-11 ч.1 ст.6

Возражение

против рекламных звонков и рассылок (ч.2 ст.15) и решений только на основе автоматизированной обработки (ст.16)

Переносимость

в России не закреплена, работает лишь к оператору под GDPR (ст.20 GDPR)

ПРИРОДА ПРАВА

Три следствия для оператора

1. основание обработки доказывает оператор, а субъект неправомерность не доказывает (ч.3 ст.9)
2. факт, дату и содержание ответа тоже доказывает оператор: неподтвержденный ответ в споре равен неответу
3. жалоба в Роскомнадзор и иск идут параллельно, и исполненное предписание не снимает риска компенсации (ст.17, ч.2 ст.24)

Пределы: права субъекта ограничивают три группы интересов: права третьих лиц, специальные режимы информации и публичный интерес. Предел подтверждают конкретной нормой и называют ее в мотивированном ответе

По GDPR у человека больше прав, чем по 152-ФЗ

Права субъекта по 152-ФЗ и дополнительные права по Конвенции 108+ и GDPR

Privacy Advocates

152-ФЗ

Права по российскому закону

- доступ к сведениям об обработке и к своим данным, ст.14
- уточнение, блокирование и уничтожение данных, ст.14
- требование прекратить обработку, ч.5.1 ст.21
- отказ от рекламных звонков, рассылок и политической агитации, ст.15
- возражение против решений только на основе автоматизированной обработки, ст.16
- обжалование действий оператора, ст.17
- возмещение убытков и компенсация морального вреда, ч.2 ст.24

\+

Конвенция 108+ и GDPR

Плюс к российскому набору

- ограничение обработки
- возражение против обработки в целом
- информирование человека об утечке его данных
- переносимость: копия данных в формате для другого сервиса
- право быть забытым, в России только к поисковикам по ст.10.3 149-ФЗ

В России: закон обязывает уведомлять об утечке Роскомнадзор, а не людей, но добровольное уведомление пострадавших работает на Компанию в спорах

Из семи сроков исполнения требований продлевают только десятидневный

Лестница значений по ст.10.1, 14, 15, 16, 20 и 21 152-ФЗ и правила счета по гл.11 ГК

Privacy Advocates

СРОК	ЧТО ИСПОЛНИТЬ	НОРМА	ПРОДЛЕНИЕ
немедленно	прекратить продвижение и политическую агитацию	ч.2 ст.15	нет
с обращения	блокировать спорные данные на период проверки	ч.1 ст.21	нет
3 раб. дн.	прекратить неправомерную обработку и передачу по ст.10.1	ч.3 ст.21, ч.14 ст.10.1	нет
7 раб. дн.	уточнить или уничтожить ПД от даты подтверждающих сведений	ч.3 ст.20, ч.2 ст.21	нет
10 раб. дн.	сведения, отказ, прекращение по требованию, ответ органу	ст.14, 20, ч.5.1 ст.21	**+5 раб. дн.**
30 дней	цель достигнута, согласие отозвано, возражение по ст.16	чч.4, 5 ст.21, ч.4 ст.16	нет
6 месяцев	предел блокирования, если уничтожить в срок нельзя	ч.6 ст.21	нет

КАК СЧИТАТЬ

отсчет со следующего дня после получения (ст.191 ГК), конец в нерабочий день переносится (ст.193 ГК). В ст.21 рабочие и календарные дни соседствуют, а согласие на распространение прекращается с поступления требования (ч.13 ст.10.1)

ПРОДЛЕНИЕ

мотив раскрывают по существу и уведомляют до истечения срока: письмо на 11-й рабочий день лишь фиксирует просрочку. 30 дней продления из 59-ФЗ к частному оператору неприменимы

Ст.16 об автоматизированных решениях требует трех условий сразу

Решение о человеке, значимые последствия и исключительный автоматизм: проверка и маршрут

Privacy Advocates

1

Есть решение

вывод о конкретном лице для действия: отказ, цена, условие доступа, категория риска

2

Последствия значимы

юридические последствия или иное затрагивание прав, включая одобрение на измененных условиях

3

Автоматизм исключителен

у человека нет всего материала и полномочия отклониться от подсказки системы

4

Вывод письменно

квалификацию фиксируют с обоснованием, проверку останавливают на первом "нет"

ЕСЛИ СТ.16 ПРИМЕНИМА, ПРОЦЕСС ВЕДУТ ПО ОДНОМУ ИЗ ЧЕТЫРЕХ МАРШРУТОВ

маршрут А

Человек в контуре

доступ к материалу, полномочие отклониться и журнал решений

маршрут Б

Письменное согласие

обособленная форма и альтернатива, в кадрах недоступен (п.6 ст.86 ТК)

маршрут В

Федеральный закон

закон разрешает решение и сам задает меры защиты прав

маршрут Г

Отказ от автоматизма

решение целиком возвращают человеку

Контекст 2026: закон об ИИ 243-ФЗ от 26.07.2026 требований к автоматизированным решениям не вводит, а рекламная сегментация ст.16 не запускает

Право на забвение и данные умерших подчиняются особым правилам

Ст.10.3 149-ФЗ для поисковиков и ч.7 ст.9 152-ФЗ для наследников: адресат, основания и проверка

Privacy Advocates

Забвение

Требование к поисковой системе

ст.10.3 149-ФЗ, вне 152-ФЗ: жалоба в Роскомнадзор по ПД предмета не создает (позиция 28.01.2022)

- адресат - оператор поисковой системы, с 01.10.2024 без рекламного признака (158-ФЗ)
- три основания: распространение с нарушением закона, недостоверность, неактуальность
- 10 рабочих дней, из выдачи убирают ссылки, а сам материал остается
- не забываются неистекшие сроки преследования и непогашенная судимость
- недостоверность доказывает заявитель, факт обращения не раскрывают

Данные умершего

Правомочия наследников

ч.7 ст.9 152-ФЗ: сведения остаются ПД, требования к обработке не смягчаются

- согласие дают наследники призванной очереди, принявшие наследство (КС, 1176-О от 30.05.2024)
- фактического принятия наследства достаточно, свидетельства не ждут
- прижизненная воля субъекта сильнее воли наследников
- изображение и частную жизнь защищают дети, супруг и родители (ст.152.1, 152.2 ГК)
- наследник не владелец данных: его согласие сверяют с интересами умершего

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
SAJ-019	Рекомендательные технологии требуют правил и уведомления	22 Сайт

17.2

Прием обращения и идентификация заявителя

- Обращение субъекта оценивают по сути просьбы, а не по заголовку
- Срок ответа считают с поступления обращения по любому каналу
- Личность заявителя проверяют данными, которые у оператора уже есть
- Представитель субъекта действует только в пределах полномочий

Обращение субъекта оценивают по сути просьбы, а не по заголовку

Одно письмо несет несколько требований, и у каждого своя норма, срок и набор реквизитов

Privacy Advocates

1 **Выписать требования**
по просительной части

2 **Назначить норму и срок**
тип дней и продление по треку

3 **Проверить адресата**
при поручении - своя часть

4 **Записать в журнал**
исполнитель по каждому треку

КАК ПИШЕТ ЗАЯВИТЕЛЬ	ЧТО ЭТО ПО ЗАКОНУ	НОРМА	РЕКВИЗИТЫ
"зачем вам мои данные"	запрос сведений	ч.7 ст.14, ч.1 ст.20	**нужны**
"исправьте мой телефон"	уточнение по подтверждающим сведениям	ч.3 ст.20, ч.2 ст.21	не нужны
"удалите мои данные"	уничтожение, отзыв или прекращение	ч.3 ст.20, чч.5, 5.1 ст.21	не нужны
"перестаньте мне звонить"	прекращение продвижения, немедленно	ч.2 ст.15	не нужны
"уберите мое фото с сайта"	прекращение передачи распространяемых ПД	ч.12 ст.10.1	свой перечень
"почему отказал алгоритм"	возражение против автоматизированного решения	чч.3, 4 ст.16	не нужны

Практика: реквизиты ч.3 ст.14 нужны только запросу сведений, а требования письма рассматривают независимо: АС Москвы отменил отказ надзора, переквалифицировавшего запрос (А40-208475/2025, первая инстанция)

Срок ответа считают с поступления обращения по любому каналу

Карта каналов, регистрация в день поступления, первая линия и запрос, пришедший обработчику

Privacy Advocates

Каналы входящего

почтовый адрес | все публичные адреса почты | адрес ответственного из реестра операторов | личный кабинет | формы на сайте | чат и колл-центр | фронт-офис | способ отзыва из текста согласия

Регистрация в день поступления

дата и время, канал, полный текст и доказательство получения: срок течет с получения, а не с регистрации

Первая линия

"удалите мои данные" в чате - требование со сроком, а не жалоба на сервис. Контакт сразу передают ответственному

Очистка до пересылки

лишние сканы и данные третьих лиц внутрь не пересылают, оригинал держат в папке с ограниченным доступом

Запрос пришел обработчику

молчать нельзя: подтвердить обработку по поручению, раскрыть свою часть и адресовать к оператору

Важно: ответ "только через личный кабинет" или "приходите с паспортом" уже отказ: АС Москвы признал требование явки нарушением ч.3 ст.14 (А40-208475/2025, первая инстанция). Дубль письма по двум каналам злоупотреблением не является, а способ отзыва в отдельном согласии с 01.09.2025 стал проверяемым каналом

Личность заявителя проверяют данными, которые у оператора уже есть

Зеркальность средств, запрет добора сведений и четыре исхода при нехватке данных

Privacy Advocates

ЗЕРКАЛЬНОСТЬ

Проверяют связь с учетной записью

- личный кабинет решил задачу входом, телефон - кодом из сообщения или контрольными вопросами
- копия паспорта у клиента, известного по номеру телефона, - сбор без основания
- ответ по одному совпадению ФИО - раскрытие ПД постороннему, то есть инцидент
- добор сведений сверх перечня с последующим согласием Роскомнадзор отверг (28.01.2022)
- опечатку в одном реквизите оценивают по всему пакету документов

ДАННЫХ НЕ ХВАТАЕТ: ДВА ВОПРОСА И ЧЕТЫРЕ ИСХОДА

меры нужны, риск высокий

Запросить недостающее

запрос о данных клиента банка без реквизитов документа

меры не нужны, риск высокий

Мотивированно отказать

бумажный запрос к онлайн-сервису без связи с учетной записью

меры не нужны, риск низкий

Исполнить

отзыв согласия на рассылку от незарегистрированного пользователя

меры нужны, риск низкий

По обстоятельствам

исполнить либо принять меры, ответ дать в пределах срока

Правило: отказ по неидентификации называет недостающий реквизит и уходит в основной срок: запрос недостающего срок не приостанавливает, а молчание равно непредоставлению сведений

Представитель субъекта действует только в пределах полномочий

Доверенность, законный представитель, адвокат и наследник: что проверить и чего не требовать

Privacy Advocates

КТО ОБРАЩАЕТСЯ	ЧЕМ ПОДТВЕРЖДАЕТ	ЧТО ПРОВЕРИТЬ	ЧЕГО НЕ ТРЕБОВАТЬ
Представитель по доверенности	простая письменная доверенность, ее может представить и сам доверитель (Минцифры, 10.07.2019)	полномочие именно на это действие: сведения, отзыв согласия и уничтожение - разные полномочия	нотариальной формы и новых сведений о представляемом
Законный представитель	свидетельство о рождении, акт о назначении опекуна или попечителя	соответствие статуса возрасту и дееспособности субъекта	документов сверх подтверждающих статус
Адвокат	адвокатский запрос с реквизитами соглашения, ордера или доверенности (приказ Минюста № 288)	режим запроса: свой срок и ответственность по ст.5.39 КоАП	данных третьих лиц, не являющихся доверителями, без их согласия (позиция Роскомнадзора 22.09.2023)
Наследник	документы о принятии наследства, в том числе фактическом	призванную очередь и линию требования: доступ или согласие на обработку	завершенного наследственного дела и свидетельства

Граница: проверка полномочий не превращается в самостоятельный сбор данных: оператору нужен документ о полномочии, а не сведения сверх необходимого для ответа

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
SAJ-010	Согласие отделяют от политики и пользовательского соглашения	22 Сайт
SAJ-014	Чем пассивнее согласие на рассылку, тем выше риск	22 Сайт

17.3

Ответ, отказ и надзорный след

- Ответ на запрос собирают по каждому пункту ч.7 ст.14
- Отказ без ссылки на норму не отказ, а просрочка
- Исполнение требования не заканчивается правкой записи
- Исполнение доказывают журналом, а не регламентом

Ответ на запрос собирают по каждому пункту ч.7 ст.14

Состав сведений, форма ответа и почему быстрая отписка хуже полного ответа в срок

Privacy Advocates

СКЕЛЕТ ОТВЕТА, Ч.7 СТ.14

По каждому пункту текст или "неприменимо"

1. подтверждение факта обработки
2. правовые основания и цели
3. способы обработки
4. лица с доступом и получатели, кроме работников
5. какие ПД заявителя и их источник
6. сроки обработки и хранения
7. порядок реализации прав
8. трансграничная передача
9. обработчик: наименование и адрес
10. меры по ст.18.1 и иные сведения по закону

Форма ответа - форма входящего

бумага на бумагу, электронный на электронный, указание заявителя обязательно (ч.3 ст.14). Требование явиться в офис образует состав ч.4 ст.13.11 КоАП

Отсылка к политике - не ответ

политика описывает обработку вообще, а заявитель спрашивает о себе. Техническая выгрузка из ИСПД доступной формой тоже не является

Полнота каждого письма

неполный ответ образует тот же состав, что молчание, и собрать полноту из нескольких писем нельзя

Быстрая отписка хуже

Второй кассационный суд признал моментом правонарушения дату неполного ответа, отправленного назавтра после запроса (№ 16-1734/2025, штраф 40 000 ₽ устоял)

Бесплатно и без "вы уже знаете"

ознакомление безвозмездно, а осведомленность заявителя из договора или кабинета основанием отказа не служит

Отказ без ссылки на норму не отказ, а просрочка

Что служит основанием отказа, что нет, и как собрать мотивированный отказ в срок ч.2 ст.20

Privacy Advocates

Работает

Основание названо законом

- ч.8 ст.14: оборона, безопасность, оперативно-разыскная деятельность, противодействие легализации и иные случаи федерального закона
- права третьих лиц: их данные маскируют, а документ выдают в части заявителя
- повторный запрос о тех же сведениях раньше 30 дней без обоснования (чч.4-6 ст.14)
- неподтвержденная личность с указанием недостающего реквизита
- иное основание из пп.2-11 ч.1 ст.6 при требовании прекратить обработку

vs

Не работает

Основание придумано оператором

- чрезмерность запроса: фильтра, как в ст.12 GDPR, в законе нет
- "сведения конфиденциальны и выдаются только по запросу суда"
- коммерческая тайна без нормы и внутренние правила оператора
- специальный статус, например финансового управляющего: обязанность ответить подтвердил 3 КСОЮ, хотя дело прекратил за давностью (16-2744/2025)
- обезличивание вместо уничтожения или прекращения обработки

Скелет отказа | дата получения | требование словами заявителя | норма с пунктом | почему норма применима | что выдается при частичном отказе | право обжаловать в Роскомнадзор или суд | подпись | отправка в 10 рабочих дней

Исполнение требования не заканчивается правкой записи

Блокирование с момента обращения, проверка основания, уведомление получателей, подтверждение исполнения

Privacy Advocates

1

Заблокировать сразу

спорные данные с момента обращения, не дожидаясь документов, и не весь массив о человеке

2

Проверить основание

уточнение - при дефекте записи, уничтожение - если ПД незаконно получены или не нужны для цели

3

Исполнить в срок трека

при ином основании из пп.2-11 ч.1 ст.6 назвать норму и срок, до которого данные хранятся

4

Уведомить получателей

субъекту - о результате, третьим лицам с прежней версией - разумными мерами (чч.1-3 ст.21)

5

Подтвердить артефактом

акт об уничтожении по приказу № 179 прикладывают к ответу, выгрузку о блокировании хранят с ним

ТРЕБОВАНИЕ РОСКОМНАДЗОРА

Исполняют наравне с требованием субъекта

санкция та же: ч.5 ст.13.11 КоАП - юрлицу 50-90 тыс. ₽, повторно по ч.5.1 - 300-500 тыс. ₽. Состав есть, только если данные обладают признаками диспозиции: апелляция отменила предупреждение ТСЖ, данные которого раскрыл сам заявитель (А56-105866/2025, 28.06.2026)

ДАННЫЕ ИЗ ГИС

Исправляют и у источника

если ошибка пришла из государственной системы, требование адресуют и ее оператору: такой маршрут Минцифры назвало для мессенджера MAX (31.08.2026)

Исполнение доказывают журналом, а не регламентом

Поля журнала обращений, сроки хранения переписки и что увидит проверяющий по входящим субъектов

Privacy Advocates

17 из 75

вопросов листа

срабатывают от входящего субъекта

2 года

переписки

копии обращений и ответов истребуют за 2 года

3 года

акт и выгрузка

хранят подтверждения уничтожения (п.8 приказа № 179)

1 год

давность

по чч.4, 5 ст.13.11 КоАП с даты неполного ответа

МИНИМАЛЬНЫЕ ПОЛЯ ЖУРНАЛА

- входящий номер, дата и время, канал
- заявитель, статус, способ проверки личности
- дословная просительная часть
- норма и срок по каждому треку
- продление с реквизитами уведомления
- исполнитель и результат по треку
- дата, способ и доказательство отправки
- уведомление третьих лиц и повторность

ТИПОВЫЕ ПРОВАЛЫ

- конвейер замкнут на клиентский сервис без ответственного
- заявителю и регулятору сообщают разные версии
- ответ хранят без акта или выгрузки
- ответ ушел почтой без доказательства

Для оператора один иск недорог, коллективные дороже и заметнее

Моральный вред по ст.24 152-ФЗ, коллективные иски после утечек и убытки за избирательные жалобы

Privacy Advocates

150 000 ₽

редкая высокая сумма

восемь сим-карт на паспорт абонента без его ведома (2-6115/2025)

5 000 ₽

из заявленных 100 000 ₽

одному истцу по массовой утечке, апелляция 01.08.2023

225 000 ₽

убытки с заявителя

за более чем 200 избирательных жалоб на одно издание (А19-1402/2024)

Обычная компенсация

реклама без согласия или нарушение права работника на информацию оцениваются порядка десяти тысяч ₽, имущественный вред почти не взыскивают

Коллективные иски

по сообщениям прессы, после утечки сервиса доставки 33 клиента заявили по 100 000 ₽: объединенное требование дает и сумму, и публичный сюжет

Для оператора: по делу о жалобах на рекламу суд счел злоупотреблением формальные, систематические и избирательные жалобы, механизм переносим на обращения в Роскомнадзор. Расходы на ответы подтверждают договорами и актами

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
NAD-010	Ответ на запрос по жалобе становится доказательством	29 РКН и органы
HRN-009	Сроки уничтожения задают 152-ФЗ, ТК, ГК и налоговые законы	18 Уничтожение ПД
HRN-012	Уничтожение подтверждают актом, а в ИСПД еще и выгрузкой	18 Уничтожение ПД

17.4

Особые субъекты

- ПД умершего не наследуют, у аккаунта и контента свои правила
- Права иностранца защищены как у гражданина, но локализация иная
- Данные иностранного работника подают в МВД по форме, без согласия
- Судимость проверяют по закону о должности, а не по согласию

ПД умершего не наследуют, у аккаунта и контента свои правила

Судьба аккаунта не урегулирована, права на контент наследуются, медкарта и счета под своими тайнами

Privacy Advocates

ЧТО ОСТАЛОСЬ	КАК РЕШАЕТСЯ	ОПОРА
Аккаунт и переписка	законом не урегулированы и спорны, на деле решают пользовательское соглашение и переданные логин и пароль	договор с площадкой
Контент и активы	наследуются исключительные права на охраняемый контент и ЦФА, а сам аккаунт нотариат объектом ИС не считает	пп.90, 91 ПП ВС № 9, 259-ФЗ, ФНП
Медицинские документы	супругу, близким родственникам по закрытому перечню и названным пациентом лицам, если нет прижизненного запрета	ч.3.1 ст.13 323-ФЗ, КС № 1-П
Сведения о счетах	выдачу распечатки матери клиента, позже принявшей наследство, апелляция сочла малозначительной, но тайну наследование не снимает	10-3796/2025, ч.2 ст.183 УК

БЕЗ СОГЛАСИЯ НАСЛЕДНИКОВ

Законный оборот

- регистрация смерти, нотариат и архив
- похоронное дело и книги захоронений
- страховые и судебные процедуры
- в объеме функции (ст.5, 7 152-ФЗ), а доступ перевозчика тел к данным умерших 4 ААС счел конкурентным преимуществом (А10-4767/2014)

Срок: охрана данных умершего бессрочна, а хранение нет. Им назначают цель, состав и срок, затем уничтожают или сдают в архив, где сведения о частной жизни закрыты 75 лет с создания документа, раньше по письменному разрешению наследников (ст.25 125-ФЗ)

Права иностранца защищены как у гражданина, но локализация иная

Национальный режим и три территориальных признака, которые для данных иностранца не совпадают

Privacy Advocates

МЕХАНИЗМ	ЧТО ВКЛЮЧАЕТ	ДАННЫЕ ИНОСТРАНЦА
Защита и права	национальный режим ч.3 ст.62 Конституции	в полном объеме
Локализация, ч.5 ст.18	сбор ПД граждан РФ	вне требования, если массив отделен
Приземление, 236-ФЗ	иностранный ресурс, из России больше 500 тыс. в сутки, ряд лиц без порога	входят наравне с данными граждан
ТПД, ст.12	получатель за рубежом	возврат в страну гражданства тоже ТПД

ГРАЖДАНСТВО НЕ ПРОВЕРИТЬ

способ выбирает оператор (Роскомнадзор 19.01.2015, Минкомсвязь 25.08.2015), по экспертному подходу поле гражданства, версия ресурса или геолокация

СПОРНО

по гражданству иностранец в России вне локализации, а по местонахождению втягивает оператора в приземление, поэтому держат оба сценария

Спецкатегория: связка гражданства, страны рождения и языка, по экспертному подходу, раскрывает национальность, а отчет о национальном составе персонала эксперты относят к спецкатегории

Данные иностранного работника подают в МВД по форме, без согласия

Уведомления работодателя по приказу МВД № 290 (с 01.09.2026 до 01.09.2032) и миграционная биометрия

Privacy Advocates

1

Договор

заключение и прекращение, 3 рабочих дня, орган по месту работы иностранца

2

Трудоустройство

подает организация по трудоустройству, по каждому иностранцу, 3 рабочих дня

3

Зарплата ВКС

ежеквартально, в орган, выдавший разрешение на работу

4

Ходатайство ВКС

подает сам иностранец с двумя согласиями, сведения видны на сайте МВД

- Форма задает состав сведений, и запрос сверх ее полей основания не имеет
- Приложенное согласие не основание, его отзыв обязанности не отменяет
- Чье это согласие, спорно, УМВД по Тюменской области (27.08.2026) за подающее лицо

МИГРАЦИОННАЯ БИОМЕТРИЯ С 29.12.2021

дактилоскопия и фото по 274-ФЗ за 30 дней у въехавших для работы и за 90 дней у въехавших не для работы на срок свыше 90 дней (п.13 ст.5 115-ФЗ). Частному оператору этот слой основания не дает

⚠ **Ошибка:** уведомления шлют по месту нахождения работодателя, хотя адресат определяется местом работы, а при патенте на два субъекта уведомляют оба органа

Судимость проверяют по закону о должности, а не по согласию

Обособленный режим ч.3 ст.10 152-ФЗ: круг операторов, состав справки, хранение и новый канал с 01.02.2027

Privacy Advocates

Ч.3 СТ.10 152-ФЗ

Закон называет оператора, а не способ

судимость обрабатывают госорганы в пределах полномочий и иные лица в случаях и порядке федеральных законов. Согласия среди условий нет, и, по экспертному подходу, подпись кандидата случая закона не создает, хотя вопрос спорен

СИТУАЦИЯ	ВЫВОД	ОПОРА
Педагог, финансы, транспорт	допустима для должности, где закон ограничивает функцию лицам с судимостью	ст.331 ТК и отраслевые нормы
Банк	только должности перечня закона о банках, для прочих анкета нарушает ч.3 ст.10	12-1517/2016
Анкета о себе и родне	нарушение ч.3 ст.10 и избыточность по ч.5 ст.5, приказ об исключении анкеты допущенную обработку не исцеляет	А55-21355/2018
Справка о судимости	по позиции Минцифры (12.10.2022) наличие и отсутствие без деталей идут по ст.6, Роскомнадзор устно (14.08.2026) наличие относит к ст.10	спорно
Бенефициары контрагента	прямой нормы о проверке их судимости нет, согласие пробел не закрывает	ч.3 ст.10 152-ФЗ

Хранение: после кадрового решения хранят факт предъявления справки с датой, номером и органом. С 01.02.2027 работодатели-юрлица в эксперименте с цифровым профилем (ПП № 710 в ред. ПП № 1217) получат сведения МВД через ЕСИА, но право на запрос дает только закон

Данные ИП остаются ПД, сведения из ЕГРИП обычно ведут без согласия

ИП и самозанятый: реестровая публичность, личный контур, деловые рассылки и спор о правах субъекта

Privacy Advocates

ИП

Реестр открыт по закону

ст.6 129-ФЗ, кроме документа о личности и места жительства

- контрагент обходится без согласия по пп.2, 5, 7 и 11 ч.1 ст.6, а удалить себя из реестра нельзя (КС, 1346-О)
- только реестровые сведения публикуют без нарушения, сверх реестра нужно основание (Роскомнадзор устно 27.08.2025)
- выгрузка и перепродажа реестра, по экспертному подходу, выходят за цель раскрытия, реестр не общедоступный источник по ст.8

Самозанятый

Открытого реестра нет

по экспертному подходу, публично виден лишь статус НПД

- ФИО и ИНН заказчик получает в чеке для учета и по договору
- ИНН и адрес отгрузки остаются личными, как у ИП без помещения
- довод о публичности не работает, статус спорен, практики нет
- с данными клиентов он, как и ИП, оператор с уведомлением (Роскомнадзор устно, 22.08.2025)

СПОРНО

Управление Роскомнадзора по ЦФО (2022, 2025) и сам Роскомнадзор устно (14.08.2026) не дают ИП в объеме ЕГРИП прав субъекта. Надежнее трактовка ПД без согласия

РАССЫЛКИ

по ст.18 закона о рекламе нужно согласие абонента, а контакты ИП с площадок Роскомнадзор устно (14.08.2026) допускает, если площадка не ограничивает

Каждое требование субъекта исполняют в срок и с доказательствами

Выводы раздела

Privacy Advocates

ГЛАВНОЕ

Право исполняют по треку, сроку и доказательству

оператор квалифицирует каждое требование, ставит ему норму и срок, отвечает полно и хранит артефакт исполнения

Квалификация первым шагом

просительную часть разбирают на требования, и каждое получает свою норму, срок и реквизиты

Лестница, а не один срок

семь значений, рабочие и календарные дни, продление до 5 рабочих дней только у десятидневных сроков

Любой канал запускает срок

карта каналов и регистрация в день поступления важнее единого окна, удобного оператору

Личность без добора

проверяют средствами, которыми оператор уже пользуется, а отказ называет недостающее

Полнота и след

ответ по ч.7 ст.14 поштучно, отказ только по норме, исполнение подтверждают актом и журналом

ЧАСТЬ

V

Хранение, локализация и передачи

Сколько хранить ПД, где их хранить и кому можно передать

18 Хранение, обезличивание и уничтожение ПД
19 Локализация баз с ПД
20 Трансграничная передача ПД
21 Поручение и передача третьим лицам

18

Хранение, обезличивание и уничтожение ПД

Сроки, архив, обезличивание и доказуемое уничтожение

18.1 Прекращение обработки и архив

18.2 Обезличивание с 01.09.2025

18.3 Сроки хранения

18.4 Подтверждение уничтожения

18.5 Способы и СЗИ

Раздел на сайте
privacy-advocates.ru/pd/hrn

18.1

Прекращение обработки и архив

- Обезличивание не входит в способы прекращения обработки
- Уничтожение необратимо, удаление и блокирование обратимы
- Архивирование переводит документы из режима ПД в режим 125-ФЗ

Обезличивание не входит в способы прекращения обработки

Уничтожение или удаление, блокирование и архивирование против обезличивания

НЕ ПРЕКРАЩАЕТ ОБРАБОТКУ

Обезличивание

способ минимизации обработки и обеспечения конфиденциальности ПД. Оно само является обработкой (п.3 ст.3 152-ФЗ), а его результат остается ПД

Уничтожение или удаление

уничтожение необратимо, удаление изымает данные из системы или с носителя с возможностью восстановления

Блокирование

временное прекращение обработки, кроме обработки, необходимой для уточнения ПД

Архивирование

перевод документов в режим архивного хранения по 125-ФЗ с собственными сроками и порядком уничтожения

Следствие: обезличивание в ответ на требование субъекта об уничтожении или на отзыв согласия требование не исполняет, а указывать его способом уничтожения в акте Роскомнадзор не разрешает

Уничтожение необратимо, удаление и блокирование обратимы

Три операции с ПД с разным результатом: дефиниции и сравнение

Privacy Advocates

п.8 ст.3 152-ФЗ

Уничтожение

действия, в результате которых невозможно восстановить содержание ПД в ИСПД и (или) уничтожаются материальные носители ПД

письмо АРБ от 02.12.2011 № 5

Удаление

изъятие ПД из ЭВМ с сохранением возможности их восстановления. Легального определения нет, Минцифры понимает удаление как исключение данных с носителя или из ИС

п.7 ст.3, ч.2 ст.21 152-ФЗ

Блокирование

временное прекращение обработки ПД, за исключением случаев, когда обработка необходима для уточнения ПД

ОПЕРАЦИЯ С ПД	ОБРАТИМОСТЬ	ДЛИТЕЛЬНОСТЬ	ДОСТУП	ЭВМ / БУМАГА
Уничтожение	необратимо*	постоянно	невозможен	да / да
Удаление	обратимо	постоянно или временно	невозможен	да / нет
Блокирование	обратимо	временно	возможен	да / да

Архивирование переводит документы из режима ПД в режим 125-ФЗ

Жизненный цикл хранения: оперативное хранение, архив и уничтожение

Privacy Advocates

Работа

Оперативное хранение

данные используются и изменяются, доступ без дополнительных ограничений

Архив

Архивное хранение

данные не используются и заблокированы, доступ по специальной процедуре

Уничтожение

Окончание хранения

подтверждение для ПД с указанием отдельных субъектов, для архивных сведений без их указания

Режим ПД

152-ФЗ

ч.7 ст.5, ч.7 ст.21 152-ФЗ, приказ Роскомнадзора от 28.10.2022 № 179

- уничтожение по достижении целей обработки
- акт и выгрузка из журнала со сведениями о субъектах

Архивный режим

125-ФЗ

п.2 ч.1 ст.4, ч.5 ст.14 125-ФЗ, приказы Росархива от 20.12.2019 № 236 и от 31.07.2023 № 77

- длительные сроки хранения документов
- уничтожение без сведений о субъектах
- нет явной обязанности уведомлять об инцидентах

Важно: режим 152-ФЗ перестает применяться к документам только после оформленной процедуры передачи в архив, а по истечении архивного срока их уничтожают по правилам архивного дела

18.2

Обезличивание с 01.09.2025

- Обезличивать можно только с основанием и методом из перечня
- Риск узнать человека по данным снижают четыре группы техник
- С 01.09.2025 обезличивание идет в двух режимах
- Пример: семь ступеней снижения идентифицирующего потенциала

Обезличивать можно только с основанием и методом из перечня

Позиция Минцифры и Роскомнадзора и два условия квалификации обработки как обезличивания

Privacy Advocates

П.9 СТ.3 152-ФЗ

Обезличивание

действия, в результате которых становится невозможным **без использования дополнительной информации** определить принадлежность ПД конкретному субъекту

- обратимо по конструкции: с дополнительной информацией данные приводятся к исходному виду
- хеш-функция не обезличивает, а служит средством криптографической защиты (письмо Роскомнадзора от 01.06.2023 № 08-45913)

Не способ прекращения обработки

по мнению Минцифры и Роскомнадзора это способ обработки и обеспечения конфиденциальности, который снижает идентифицирующий потенциал ПД

Условие 1. Основание

согласие субъекта на обезличивание или иное основание из ч.1 ст.6 152-ФЗ

Условие 2. Метод

метод или комбинация методов из закрытого перечня приказа Роскомнадзора от 19.06.2025 № 140

МЕТОДЫ ПРИКАЗА № 140 С 01.09.2025

введение идентификаторов | **изменение состава или семантики** | **декомпозиция** | **перемешивание** | **обобщение, новый метод**

Схема обезличивания
скачать

Риск узнать человека по данным снижают четыре группы техник

Международная схема: от идентификационных через псевдонимные к анонимным данным

Privacy Advocates

Идентификационные данные

Прямые идентификаторы на месте

прямые идентификаторы нетронуты или частично маскированы, косвенные нетронуты

Псевдонимные данные

Прямые идентификаторы скрыты

прямые идентификаторы удалены или изменены, косвенные нетронуты

Анонимные данные

Идентификаторов нет

все идентификаторы удалены, чтобы разорвать связь данных с человеком

1

Псевдонимизация

введение случайных идентификаторов, хеширование, шифрование

2

Анонимизация через обобщение

агрегирование (обобщение) значений

3

Анонимизация через рандомизацию

добавление шума, перестановка данных или удаление атрибутов

4

Обобщение и рандомизация

сочетание нескольких техник

В российском праве: хеширование и шифрование в закрытый перечень приказа № 140 не входят, понятия анонимизации в законе нет, и Роскомнадзор оценивает любое преобразование как обезличивание

С 01.09.2025 обезличивание идет в двух режимах

Общий режим приказа Роскомнадзора № 140 и режим составов данных по ст.13.1 152-ФЗ и ПП-1154

Privacy Advocates

Общий режим

Приказ Роскомнадзора от 19.06.2025 № 140

заменил приказ № 996 от 05.09.2013, действует с 01.09.2025

- обязателен для всех операторов, которые обезличивают ПД по своим основаниям, а не только для госорганов
- закрытый перечень: четыре метода, к которым в дополнение допускается обобщение (агрегация)
- локальные акты, оценка достаточности метода, раздельное хранение массивов и ключа, учет операций
- результат остается ПД и по конструкции обратим

vs

Режим составов данных

Ст.13.1 152-ФЗ и ПП-1154 от 01.08.2025

ст.13.1 введена 233-ФЗ от 08.08.2024, режим действует с 01.09.2025

- только по адресному требованию Минцифры в случаях из перечня Правительства (ПП-538 от 24.04.2025)
- пять методов ПП-1154: введение идентификаторов, изменение состава или семантики, декомпозиция, перемешивание, преобразование
- оператор исключает сведения ограниченного доступа, составы не формируются из спецкатегорий, кроме сведений о здоровье, и биометрии
- результат передается в ГИС "Единая информационная платформа национальной системы управления данными"

Важно: для всех операторов обязательны требования к обезличиванию, а не само обезличивание. Обезличить ПД оператор обязан по требованию Минцифры и при обработке в статистических или исследовательских целях без согласия (п.9 ч.1 ст.6)

Пример: семь ступеней снижения идентифицирующего потенциала

Как меняются прямые и косвенные идентификаторы одной записи

Privacy Advocates

СТУПЕНЬ	ДАННЫЕ	ПРЯМЫЕ ИДЕНТИФИКАТОРЫ	КОСВЕННЫЕ ИДЕНТИФИКАТОРЫ	ТЕХНИКА
Беспрепятственная идентификация	идентификационные	ФИО: Мунтян Алексей Витальевич, СНИЛС: 123-456-789 01	возраст: 39 лет, IP-адрес: 192.168.0.1	техники не используются
Деперсонификация	идентификационные	ФИО: Мунтян А. В., СНИЛС: 123-456-789 01	возраст: 39 лет, IP-адрес: 192.168.0.1	редуцирование ФИО
Усиленная деперсонификация	идентификационные	ФИО: Мунтян А. В., СНИЛС: *****67890	возраст: 39 лет, IP-адрес: 192.168.0.1	маскирование СНИЛС
Псевдонимизация	псевдонимные	ФИО: 5L7T-LX619Z, СНИЛС: *****67890	возраст: 39 лет, IP-адрес: 192.168.0.1	искусственный идентификатор (псевдоним) вместо ФИО
Усиленная псевдонимизация	псевдонимные	ФИО: 5L7T-LX619Z, СНИЛС: d5efe83e	возраст: 39 лет, IP-адрес: 192.168.0.1	защита СНИЛС хешированием
Деидентификация	псевдонимные	удалены	возраст: 30-40 лет, IP-адрес: 252.112.1.90	удаление прямых идентификаторов, обобщение возраста, замена IP-адреса
Анонимизация	анонимные	удалены	удалены	удаление косвенных идентификаторов и добавление шума

18.3

Сроки хранения

- Семь событий обязывают прекратить хранение ПД
- Сроки уничтожения задают 152-ФЗ, ТК, ГК и налоговые законы
- Уничтожение срывают размытые сроки и забытые копии баз
- Биометрию уничтожают по особым основаниям 572-ФЗ

Семь событий обязывают прекратить хранение ПД

Принцип ограничения хранения по ч.7 ст.5 152-ФЗ

Privacy Advocates

ПД хранятся не дольше, чем этого требуют цели обработки, и уничтожаются по достижении целей или при утрате необходимости в них (ч.7 ст.5)

Цель достигнута	достигнуты цели обработки ПД и (или) истекли максимальные сроки хранения
Цель не нужна	утрачена необходимость в достижении целей обработки ПД
Сведения субъекта	субъект подтвердил, что ПД незаконно получены или не нужны для цели обработки
Неправомерность	невозможно обеспечить правомерность обработки ПД
Отзыв согласия	субъект отозвал согласие, а сохранение ПД для целей обработки больше не требуется
Исковая давность	истекли сроки исковой давности по правоотношениям, в рамках которых шла обработка
Ликвидация	ликвидация или некоторые формы реорганизации оператора

Сроки уничтожения задают 152-ФЗ, ТК, ГК и налоговые законы

Ориентиры для политики сроков хранения ПД

Privacy Advocates

СРОКИ 152-ФЗ

7 раб. дн. — **Сведения субъекта, ч.3 ст.20**
ПД незаконно получены или не нужны для цели

10 раб. дн. — **Неправомерная обработка, ч.3 ст.21**
обеспечить правомерность невозможно

10+5 раб. дн. — **Требование субъекта, ч.5.1 ст.21**
о прекращении обработки ПД

30 дней — **Достижение цели, ч.4 ст.21**
или утрата необходимости в ее достижении

30 дней — **Отзыв согласия, ч.5 ст.21**
если ПД больше не нужны для целей

6 месяцев — **Блокирование, ч.6 ст.21**
если своевременно уничтожить ПД невозможно

ДАВНОСТЬ И УЧЕТ

3 месяца
трудовые споры, в том числе о моральном вреде за нарушение правил обработки ПД работника, ч.1 ст.392 ТК

1 год
споры о невыплате зарплаты и о возмещении ущерба работником, ст.392 ТК

3 года
общая исковая давность (ст.196 ГК) со дня, когда узнали о нарушении (ст.200 ГК), для договора ориентир его прекращение

5 лет
для первичных учетных документов после отчетного года (ст.29 402-ФЗ) и налоговых (ст.23-24 НК), по страховым взносам 6 лет

Иные сроки
например более 5 лет, если срок проходит тест "почему именно такой?"

Уничтожение срывают размытые сроки и забытые копии баз

Две зоны трудностей: график уничтожения и периметр баз данных

Privacy Advocates

ГРАФИК УНИЧТОЖЕНИЯ

фактический срок | желаемый срок | законный срок | установленный срок | триггеры и периоды

Карта данных

по каждой категории ПД фиксирует все места хранения, срок, триггер и способ уничтожения

Срок в настройках

срок из локального акта должен быть настроен в самой системе, иначе записи живут до заполнения диска

БАЗЫ ДАННЫХ

основные и резервные | разработки | тестирования | логирования

Резервные копии

восстановление из копии возвращает уничтоженные записи, поэтому его сверяют с журналом исполненных уничтожений

Журналы

перезапись логов с ПД, по позиции Роскомнадзора от 27.08.2025, подтверждают по приказу № 179

Риск: записи с истекшим сроком, оставшиеся в резервных копиях, тестовых средах и журналах, при утечке увеличивают число затронутых субъектов и тяжесть ответственности

Биометрию уничтожают по особым основаниям 572-ФЗ

Основания уничтожения биометрических ПД и векторов ЕБС

Privacy Advocates

п.5 ч.14, ч.15 ст.3

Отзыв согласия

субъект отозвал согласие на обработку биометрических ПД

п.6 ч.14, ч.15 ст.3

Требование субъекта

об уничтожении биометрических ПД и (или) векторов ЕБС

ч.14 ст.4, ч.3 ст.26

Размещение в ЕБС

биометрические ПД уничтожаются в информационных системах организаций

ч.7 ст.14, п.3 ч.1 и ч.2 ст.15

10 суток вне ЕБС

истек срок хранения биометрических ПД для рассмотрения обращений субъектов

ч.15 ст.16

Запрос оператора ЕБС

мотивированный запрос об уничтожении векторов ЕБС

п.6 ч.2 ст.8, п.7 ч.8 ст.5

Запрос уполномоченного органа

мотивированный запрос Роскомнадзора к оператору ЕБС или регионального сегмента

Вне ЕБС: по истечении срока хранения организация, осуществляющая аутентификацию, уничтожает биометрические ПД средствами защиты, прошедшими оценку соответствия, с функцией автоматического уничтожения по истечении заданного срока (ч.2 ст.15)

18.4

Подтверждение уничтожения

- Уничтожение подтверждают актом, а в ИСПД еще и выгрузкой
- Роскомнадзор: выгрузка не заменяет акт, ФИО в акте обязательны
- Длинный список субъектов в акте заменяют файлом с хешем
- Акт и выгрузку хранят 3 года, и это не архивный срок

Уничтожение подтверждают актом, а в ИСПД еще и выгрузкой

Реквизиты по требованиям приказа Роскомнадзора от 28.10.2022 № 179

Privacy Advocates

АКТ ОБ УНИЧТОЖЕНИИ ПД

- наименование или ФИО и адрес оператора
- наименование или ФИО и адрес обработчика при поручении обработки
- ФИО или иные идентификаторы субъектов, ПД которых уничтожены
- ФИО, должности и подписи уничтоживших, подпись собственноручная или электронная
- перечень категорий уничтоженных ПД
- наименование и число листов носителя при неавтоматизированной обработке
- наименование ИСПД при автоматизированной обработке
- способ уничтожения
- причина уничтожения
- дата уничтожения

ВЫГРУЗКА ИЗ ЖУРНАЛА РЕГИСТРАЦИИ СОБЫТИЙ В ИСПД

Пять сведений

выгружается при уничтожении ПД в ИСПД

- ФИО или иные идентификаторы субъектов
- перечень категорий уничтоженных ПД
- наименование ИСПД
- причина уничтожения
- дата уничтожения

Порядок: акт составляют при уничтожении и на материальных носителях, и в ИСПД, одной выгрузки мало (письмо Роскомнадзора от 15.03.2023 № 08-21165). Недостающие в выгрузке сведения вносят в акт, оба документа хранят 3 года

Роскомнадзор: выгрузка не заменяет акт, ФИО в акте обязательны

Разъяснения регулятора к приказу № 179

Privacy Advocates

? Заменяет ли выгрузка из журнала акт?

нет, выгрузка подтверждает уничтожение ПД, обрабатываемых с использованием средств автоматизации, и не подменяет необходимость составить акт

? Куда вносить то, чего нет в выгрузке?

сведения, которые технически нельзя реализовать в выгрузке из журнала регистрации событий, отражают в акте об уничтожении

? Обязательны ли ФИО субъектов в акте?

да, если ФИО субъектов есть у оператора

? Когда в акте указывают иную информацию?

когда ФИО субъекта у оператора нет: тогда приводят конкретные идентификаторы (атрибуты), относящиеся к лицу

? Действует ли приказ для архивных документов?

нет, он не распространяется на хранение, комплектование, учет и использование документов Архивного фонда РФ и других архивных документов

Длинный список субъектов в акте заменяют файлом с хешем

Два шаблона акта: об уничтожении ПД и об уничтожении материальных носителей

Privacy Advocates

Шаблон 1

Акт об уничтожении (прекращении обработки) ПД

- комиссия из председателя и двух членов отбирает ПД, цели обработки которых достигнуты или утратили необходимость
- таблица из 9 граф: носитель, его тип и регистрационный номер, ФИО субъекта, категории ПД, ИСПД, способ и причина уничтожения
- носители сверяют с актом, уничтожают или возвращают для повторного использования и списывают с журналов учета

Шаблон 2

Акт об уничтожении материальных носителей с ПД

- перечень носителей, например письменных согласий, выносят в электронный файл
- файл идентифицируют по имени, размеру в байтах и хеш-суммам по алгоритмам MD5 и SHA-1
- файл записывают на компакт-диск, который хранится вместе с актом

Также: акт допустимо составить в электронной форме и подписать любым видом электронной подписи (письмо Роскомнадзора от 27.12.2022 № 08-115265), а хеш служит контролю целостности и обезличиванием не является

Акт и выгрузку хранят 3 года, и это не архивный срок

Росархив о соотношении п.8 приказа № 179 и законодательства об архивном деле

Privacy Advocates

При определении сроков хранения актов об уничтожении персональных данных и выгрузки из журнала регистрации событий в информационной системе персональных данных следует руководствоваться пунктом 8 Требований, что не противоречит части 1 статьи 21.1 Закона об архивном деле

Росархив, письмо от 16.10.2024 № Р/П-448

ВОПРОС

1. п.8 приказа № 179 требует хранить акт и выгрузку 3 года с момента уничтожения, а Перечень ТУАД (приказ Росархива № 236) таких документов не упоминает
2. считать ли 3 года архивным сроком и сколько хранить документы после него

ПОЧЕМУ ТАК

1. приказ № 179 не распространяется на документы архивного хранения (п.2 ч.2 ст.1 152-ФЗ)
2. акты и выгрузки не включены в проект ведомственного перечня Роскомнадзора

Способ уничтожения оператор выбирает под вид носителя

Типовые способы для бумажных и машинных носителей

Privacy Advocates

ЛОКАЛЬНЫЙ АКТ

Выбор за оператором

оператор определяет способы уничтожения ПД и фиксирует порядок в локальном акте, а способ каждой операции указывает в акте об уничтожении

- проверка одна: содержание не восстанавливается доступными нарушителю средствами

БУМАЖНЫЕ НОСИТЕЛИ

- вымарывание или удаление данных
- разрезание носителя
- сжигание носителя
- измельчение носителя
- сдача на утилизацию вторсырья

МАШИННЫЕ НОСИТЕЛИ

- механическое уничтожение носителя
- стирание данных штатным ПО
- стирание специализированным ПО или устройствами
- нарушение функциональных возможностей носителя
- сдача на утилизацию вторсырья

В ИСПД: для машинных носителей п.3.1 ч.2 ст.19 152-ФЗ требует СЗИ с функцией уничтожения и оценкой соответствия

18.5

Способы и СЗИ

- ПП-226 добавило в ПП-1233 уничтожение электронных ДСП
- СЗИ для уничтожения требует норма о безопасности, а не ст.21
- Минцифры и Роскомнадзор отослали вопрос о СЗИ к ФСТЭК и ФСБ
- СЗИ для уничтожения нужны, если их требуют актуальные угрозы

ПП-226 добавило в ПП-1233 уничтожение электронных ДСП

Уничтожение по п.2.6 Положения о служебной информации ограниченного распространения в редакции от 04.03.2026

Privacy Advocates

01

Порядок и основание

локальные акты по правилам работы с документами Архивного фонда, основание - акт о выделении документов к уничтожению

02

Бумажные носители

шредирование или иной способ, исключающий восстановление содержания, с отметками в учетных формах

03

Электронные документы

сертифицированные устройства уничтожения, нарушение целостности носителя либо удаление остаточной информации

Обязательно

Госсектор

ФОИВ, органы по атомной энергии и космической деятельности и подведомственные им организации (п.1.1). Порядок определяет руководитель (п.1.5), нарушители отвечают (п.1.8)

Рекомендация

Остальные

органы субъектов и МСУ, госучреждения, ГУП, МУП, юрлица с госучастием и иные юрлица (п.3 постановления), ответственности за неисполнение нет

Для ПД: документы ДСП обычно содержат ПД, поэтому в госсекторе к приказу № 179 и п.3.1 ч.2 ст.19 152-ФЗ добавляется порядок ПП-1233, а для бизнеса это ориентир и возможное требование госзаказчика

СЗИ для уничтожения требует норма о безопасности, а не ст.21

П.3.1 ч.2 ст.19 152-ФЗ, введенный 233-ФЗ от 08.08.2024, и его особенности

Privacy Advocates

233-ФЗ ОТ 08.08.2024

П.3.1 ч.2 ст.19 152-ФЗ

безопасность ПД обеспечивается применением для уничтожения ПД прошедших в установленном порядке процедуру оценки соответствия СЗИ, в составе которых реализована функция уничтожения информации

1. **Только автоматизация**
   требование не распространяется на обработку ПД без использования средств автоматизации
2. **Мера безопасности**
   это мера ст.19, а не мера по выполнению обязанностей оператора (ст.18.1) и не обязанность по надлежащему уничтожению (ст.21)
3. **Вне компетенции**
   Минцифры и Роскомнадзор не отнесли вопрос к своей компетенции
4. **Ответственность**
   невыполнение квалифицируется по ст.13.12 КоАП, а не по ст.13.11

Надзор: п.33 проверочного листа (приказ Роскомнадзора от 24.12.2021 № 253) проверяет лишь организационные меры по ч.1 ст.19, технические меры по ч.2 ст.19 Роскомнадзор не проверяет. Форму листа меняет проект Роскомнадзора от 03.08.2026

Минцифры и Роскомнадзор отослали вопрос о СЗИ к ФСТЭК и ФСБ

Ответы на обращение о п.3.1 ч.2 ст.19 152-ФЗ, сентябрь 2024

Privacy Advocates

> Полагаем, что вопрос, поставленный в Вашем обращении, относится к компетенции указанных федеральных органов исполнительной власти

Роскомнадзор, письмо от 12.09.2024 № 08-377683, о ФСБ России и ФСТЭК России

РОСКОМНАДЗОР

контроль и надзор за выполнением мер ст.19 152-ФЗ осуществляют ФСБ и ФСТЭК в пределах полномочий

МИНЦИФРЫ

письмом № П25-21859-ОГ от 10.09.2024 перенаправило обращение по принадлежности (ч.3 ст.8 59-ФЗ)

ЧТО В ЗАКОНЕ

ФСБ и ФСТЭК контролируют меры ст.19 в государственных ИСПД (ч.8 ст.19), в иных системах только по решению Правительства (ч.9 ст.19)

СЗИ для уничтожения нужны, если их требуют актуальные угрозы

ПП-1119, приказ ФСТЭК № 21 и формы оценки соответствия по 184-ФЗ

Privacy Advocates

1. **Выбор СЗИ**

   оператор выбирает СЗИ по актам ФСБ и ФСТЭК, принятым во исполнение ч.4 ст.19 152-ФЗ (п.4 ПП-1119 от 01.11.2012)

2. **Когда нужна оценка соответствия**

   для всех уровней защищенности СЗИ с оценкой соответствия применяют, когда они необходимы для нейтрализации актуальных угроз (пп."г" п.13 ПП-1119, п.4 приказа ФСТЭК от 18.02.2013 № 21)

3. **Форма оценки**

   государственный контроль (надзор), испытания, регистрация, подтверждение соответствия, приемка и ввод в эксплуатацию объекта или иная форма (ч.3 ст.7 184-ФЗ)

4. **Расхождение регуляторов**

   ФСТЭК допускает СЗИ с оценкой соответствия в формах 184-ФЗ, ФСБ - только СЗИ, сертифицированные по требованиям ФСТЭК и ФСБ

РАЗДЕЛ 4 ПРИЛОЖЕНИЯ К ПРИКАЗУ № 21

ЗНИ.8 - единственная мера уничтожения

уничтожение (стирание) или обезличивание ПД на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания

- машинные носители - средства обработки (хранения) ПД и съемные машинные носители ПД (п.8.4 приказа № 21)

ФСТЭК допускает любую форму оценки, ФСБ - только сертификат

Ответы регуляторов о средствах уничтожения ПД, октябрь 2024

Privacy Advocates

ФСТЭК России

Любая форма оценки соответствия

письмо от 04.10.2024 № 240/24/4419

- меру ЗНИ.8 реализуют только СЗИ с функцией уничтожения (стирания), прошедшие оценку соответствия в любой из форм 184-ФЗ
- такие СЗИ обязательны, когда нужны для нейтрализации актуальных угроз по ПП-1119 и приказу № 21

vs

ФСБ России, 8 Центр

Только сертифицированные СЗИ

письмо от 05.10.2024 № 149/7/2/6-2076

- уничтожать ПД можно только СЗИ с функцией уничтожения, сертифицированными по требованиям ФСТЭК и ФСБ
- использование иных средств для уничтожения ПД не допускается
- если имеющиеся средства не подходят, их разработку можно заказать у лицензиатов

Выбор: оператору вне госсектора без СКЗИ ориентиром служит позиция ФСТЭК, а применяющему СКЗИ и госсектору безопаснее сертифицированное средство, которое закрывает обе позиции

Функцию уничтожения реализуют сертифицированные ПО, ПАК и ОС

Примеры СЗИ из Государственного реестра сертифицированных средств защиты информации ФСТЭК

Privacy Advocates

ПО, ООО "КОД БЕЗОПАСНОСТИ"

Secret Net Studio

функция уничтожения данных безвозвратно затирает всю информацию, включая таблицу разделов, логические тома, файловые объекты и остаточную информацию, на локальных дисках защищаемого компьютера, кроме системного, и на подключенных сменных носителях

TERRIER версия 3.0

ПО, АО "ЦБИ-сервис". Программа поиска и гарантированного уничтожения информации на дисках, средство защиты и контроля эффективности СЗИ, сертифицированное ФСТЭК России

Прибой Модуль-3.5

ПАК, ООО "Компьютерные сервисные устройства"

Стек-НСЗ

ПАК, ООО "Анна"

Astra Linux Special Edition

пример ОС с механизмом гарантированного уничтожения: очищает освобождаемую внешнюю память, чтобы удаленные файлы нельзя было восстановить

Гарантированное уничтожение перезаписывает блоки данных

Почему обычное удаление файла оставляет содержимое восстановимым: пример Astra Linux SE

Privacy Advocates

В Astra Linux Special Edition для предотвращения утечки конфиденциальных данных при восстановлении удаленных файлов реализована очистка освобождаемой внешней памяти

СОСТОЯНИЕ ФАЙЛА	БЛОКИ МЕТАДАННЫХ	БЛОКИ ДАННЫХ	ИТОГ
Файл с данными	индексные дескрипторы указывают на блоки данных	конфиденциальные данные	данные доступны
Обычное удаление	метаданные помечаются как неиспользуемые	конфиденциальные данные остаются на месте	можно восстановить
Гарантированное уничтожение	метаданные помечаются как неиспользуемые	блоки данных перезаписываются другой информацией	восстановить нельзя

Вывод: пока блоки данных не перезаписаны, удаление файла средствами ОС остается удалением, а не уничтожением по п.8 ст.3 152-ФЗ

19

Локализация баз с ПД

Рациональный подход: требование, практика и стратегии соответствия

19.1 Требование локализации

19.2 Практика 2016-2026

19.3 Какие базы локализовать

19.4 Стратегии и экономика

19.5 Кейс whistleblowing-платформы

Раздел на сайте

privacy-advocates.ru/pd/lok

РАЗДЕЛ 19. ЛОКАЛИЗАЦИЯ БАЗ С ПД

19.1

Требование локализации

Норма, ее эволюция и чтение регуляторами в 2025-2026 годах

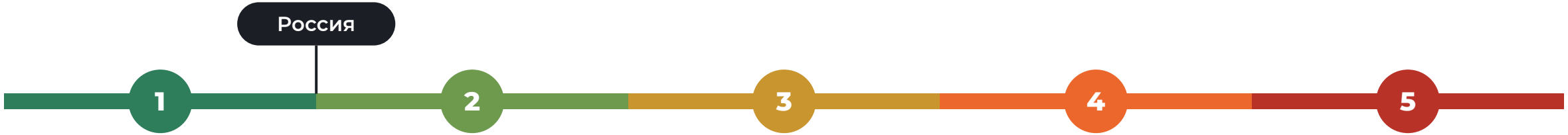
- мировой контекст и карта российских норм
- реформа 23-ФЗ и позиции РКН и Минцифры
- граница локализации и ТПД

Мировой опыт: пять моделей локализации

От мягкой к жесткой: российская модель ближе к мягким

Калькулятор локализации
скачать

Privacy Advocates



1 Локальная репликация

Local data mirroring

Копия данных хранится в стране, передача за рубеж разрешена.

2 Локальное хранение

Explicit local data storage

Данные физически остаются в стране, трансграничный доступ для обработки возможен.

3 Вынужденная локализация

De facto local storage and processing

Строгий режим передачи и крупные штрафы делают вывоз данных неприемлемым риском.

4 Хранение и обработка в стране

Explicit local storage and processing

Государство прямо запрещает трансграничную передачу.

5 Дискриминационная локализация

Discriminatory localization

Лицензирование и сертификация отсекают иностранные компании от обработки.

ГДЕ РОССИЯ

Между первой и второй моделью

Первичный контур сбора привязан к базам в РФ (ч.5 ст.18 152-ФЗ), вывоз после сбора возможен по правилам ТПД (ст.12). Полного запрета передачи нет.

82

страны с требованиями локализации в 2025 году, в 2017 - 35

214

требований в мире, в 2017 - 67

10

требований в России: третье место после Китая (33) и Индии (15)

Локализация данных в РФ: карта норм

Ядро - ч.5 ст.18 152-ФЗ, отраслевые режимы действуют наряду с ним

Privacy Advocates

ч.5 ст.18

152-ФЗ, с 01.07.2025

При сборе ПД запись, систематизация, накопление, хранение, уточнение и извлечение ПД граждан РФ с использованием баз за пределами РФ не допускаются, кроме случаев пп.2, 3, 4, 8 ч.1 ст.6. Зеркало - п.7 ч.4 ст.16 149-ФЗ, принуждение иностранных лиц - ч.4 ст.10, ст.16 236-ФЗ.

Сообщения и метаданные

ст.64 126-ФЗ
операторы связи: сообщения до 6 месяцев, сведения о фактах передачи до 3 лет

ч.3 ст.10.1 149-ФЗ
организаторы распространения информации: сообщения до 6 месяцев, сведения о фактах до 1 года

Технические средства и инфраструктура

ч.2.1 ст.13 149-ФЗ, ПП-675
средства ИС госсектора в РФ, запрет зарубежных баз для ГИС и закупщиков по 223-ФЗ

п.5 ст.29.1 закона 4015-1
технические средства страховщика

п.3 ч.3 ст.14 580-ФЗ
базы и средства службы заказа такси

подп.ж п.9 ПП-1393
инфраструктура систем оформления авиаперевозок

п.31 приказа ФСТЭК № 239
средства значимых объектов КИИ 1 и 2 категорий

243-ФЗ, с 01.03.2027
суверенные и национальные модели ИИ: ЦОД российских юрлиц

Отраслевая информация и документы

п.6 ст.4 87-ФЗ, ПП-1317
экспедитор хранит информацию о договорах 3 года

ст.12.1 381-ФЗ
исследования товарных рынков

п.25 ФСБУ 27/2021
документы и базы бухгалтерского учета

проект № 1205301-8
обработка и хранение навигационной информации о движении транспорта, первое чтение 22.10.2026

Эволюция требования о локализации

От обязанности обеспечить российские базы к запрету зарубежных

Privacy Advocates

21.07.2014 — 242-ФЗ
Введены ч.5 ст.18 152-ФЗ и п.7 ч.4 ст.16 149-ФЗ

01.09.2015 — СТАРТ
Оператор обязан обеспечить операции с ПД граждан РФ в базах на территории РФ

01.09.2022 — 266-ФЗ
Условие о локализации в поручении, иностранный обработчик отвечает наравне с оператором

01.07.2025 — 23-ФЗ
Безличный запрет операций при сборе с использованием зарубежных баз

2026 — ПРАКТИКА
Состав ч.8 ст.13.11 не изменен, дела вернулись в суды общей юрисдикции (508-ФЗ)

ДО 01.07.2025

При сборе ПД, в том числе посредством сети Интернет, **оператор обязан обеспечить** запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение ПД граждан РФ с использованием баз данных, **находящихся на территории РФ**, за исключением случаев пп.2, 3, 4, 8 ч.1 ст.6.

С 01.07.2025

При сборе ПД, в том числе посредством сети Интернет, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПД граждан РФ с использованием баз данных, **находящихся за пределами территории РФ, не допускаются**, за исключением случаев пп.2, 3, 4, 8 ч.1 ст.6.

Впереди: с 01.03.2027 суверенные модели ИИ работают только в ЦОД российских юрлиц (243-ФЗ)

Комментарии к локализации 2.0

Публичные высказывания законодателей толковательной силы не имеют

Privacy Advocates

> С 1 июля ПД россиян запрещено накапливать, хранить, обновлять в любых базах за пределами РФ. Прежнее регулирование позволяло хранить и обрабатывать такие данные в том числе за рубежом, что создавало предпосылки к их утечке.

Дмитрий Григоренко
вице-премьер Правительства РФ

строгое прочтение

АШ

Артем Шейкин
сенатор, Совет по цифровой экономике при СФ

строгое прочтение

Теперь за рубежом не должно быть даже копий баз с ПД россиян. Компании, которые вели такие операции в зарубежных БД, должны использовать инфраструктуру в РФ.

АН

Антон Немкин
член комитета ГД по информационной политике

строгое прочтение

Это элемент стратегии цифрового суверенитета. У зарубежных сервисов выбор: либо локализовать инфраструктуру в России, либо покинуть рынок.

ВБ

Владимир Булавин
глава комитета СФ по обороне и безопасности

мягкое прочтение

Это не абсолютный запрет на любую ТПД, а уточнение правил первичной обработки и хранения. Передача ПД за рубеж после их локализации в России не исключается.

Новая редакция ч.5 ст.18 внесена ко второму чтению 23-ФЗ, пояснительная записка ее цели не раскрывает. Три из четырех комментариев читают норму строго.

Интерпретация Роскомнадзором локализации 2.0

Письма РКН от 24.03.2025 № 08-134789 и от 10.04.2025 № 08-169079

Privacy Advocates

ОПЕРАТОРЫ СПРАШИВАЮТ

В какой момент оператор может считать сбор ПД завершенным?

Какое прочтение новой ч.5 ст.18 корректно?

а) уточняет прежнее требование при сборе и не запрещает последующую ТПД по ст.12

б) вводит новый запрет на зарубежные базы и при сборе, и после локализации

Письмо РКН № 08-134789
от 24.03.2025

Письмо РКН № 08-169079
от 10.04.2025

Практический смысл: сначала первичная запись и обновление в базе в РФ, затем передача другому лицу по ст.12 с уведомлением о намерении.

РОСКОМНАДЗОР ОТВЕЧАЕТ

Ограничения на ТПД ПД, ранее собранных с использованием баз в РФ, в случаях ч.1 ст.6 152-ФЗ нормой ч.5 ст.18 не устанавливаются. **Ст.12 и уведомление о намерении сохраняются.**

Позиции регуляторов 2025-2026

Ориентиры даются письмами и устно, вектор - к строгому прочтению

Privacy Advocates

24.03.2025 РКН, письма 08-134789 и 08-169079 — допускает

ч.5 ст.18 не ограничивает ТПД ПД, ранее собранных в российских базах, ст.12 сохраняется

12.05.2025 Минцифры, П25-44929 — ужесточает

уточнение и хранение ПД граждан РФ, в том числе копий, ведутся в российских базах

04.08.2025 РКН, 08-373883 — уточняет

зарубежные метрики - ТПД, допустима при соблюдении ч.5 ст.18 и ст.12

26.09.2025 Управление РКН по Пермскому краю — уточняет

сервисы Google - не ТПД, но требуют соблюдения локализации

22.10.2025 РКН, устно — ужесточает

параллельный сбор в российскую и иностранную базы недопустим

01.11.2025 РКН, ответ — уточняет

Google-таблицы с ранее собранными в РФ ПД - не ТПД, уведомление не рассматривается

12.01.2026 РКН, требование о принятии мер — ужесточает

использование Google-таблиц нарушает ч.5 ст.18 и влечет ч.8 ст.13.11 КоАП

22.01.2026 РКН, ответ — ужесточает

формы, чат-боты и скрипты, отправляющие ПД за рубеж до записи в РФ, нарушают закон

14.08.2026 РКН, день открытых дверей — ужесточает

хранение или обработка за рубежом собранных и локализованных ПД тем же оператором - не ТПД, а нарушение ч.5 ст.18

Итог: ТПД ранее собранных ПД другому лицу допустима, но зарубежный двойник российской базы у того же оператора - зона нарушения

Компромиссная интерпретация локализации 2.0

Операции с ПД по ч.5 ст.18 152-ФЗ до и после 01.07.2025

Privacy Advocates

Операция	до 01.07.2025	с 01.07.2025	Опора
ТПД ПД, собранных в российских базах, другому лицу по правилам ст.12 с уведомлением о намерении	✓	✓	письма РКН 24.03 и 10.04.2025
Сбор и обновление собранных ПД в зарубежных базах первичная запись, параллельный сбор, реплика в РФ	✗	✗	ч.5 ст.18, РКН 22.10.2025 устно
Хранение собранных ПД за рубежом тем же оператором копии, снимки, бэкапы, площадки восстановления	?	✗	Минцифры 12.05.2025, РКН 14.08.2026 устно
Иностранные офисные облака с ПД граждан РФ Google-таблицы и аналогичные сервисы	?	✗	требование РКН 12.01.2026
Генерация ПД и их хранение за рубежом производные, назначенные, предполагаемые, инициированные ПД	✓	✓	экспертный подход, Минкомсвязь 25.08.2015

Собранные ПД: получены от субъектов или представителей, взяты из открытых источников, зафиксированы отслеживанием поведения. **Сгенерированные:** получены от других лиц, образованы действиями в отношении субъекта, присвоены, синтезированы или спрогнозированы.

Общие выводы по локализации 2.0

Что изменилось к настоящему моменту

Privacy Advocates

01

Ядро не изменилось

Локализуется первичный контур сбора, а ТПД ранее собранных ПД другому лицу допустима по ст.12.

02

Двойников быть не должно

Копии, реплики и бэкапы собранных ПД за рубежом у того же оператора - зона нарушения по позиции Минцифры и РКН.

03

Точка завершения сбора

Ее нужно обосновать заранее и доказуемо: российская база как элемент ИСПД в РФ плюс журналы.

04

Иностранные облака вне процессов с ПД

Сервисы, владельцы которых привлекались по чч.8, 9 ст.13.11, исключаются из обработки ПД граждан РФ.

ЧТО СДЕЛАТЬ СЕЙЧАС

- ✓ Пересобрать карту баз первичного контура с местом размещения
- ✓ Проверить зарубежные копии, бэкапы и площадки восстановления
- ✓ Исключить иностранные офисные облака из процессов с ПД
- ✓ Проверить страницы сбора на формы, метрики, капчи и чат-боты
- ✓ Обновить поручения, заключенные до 01.07.2025

От локализации баз к приземлению обработки

Требование смещается от места данных к происхождению инфраструктуры и ПО

Privacy Advocates

Практический вывод: стратегию соответствия закладывают с запасом. Перенос одной базы при зарубежной платформе решает сегодняшнюю задачу и не решает завтрашнюю.

2015
Базы данных

Первичный контур сбора ПД граждан РФ в базах на территории РФ, ч.5 ст.18 152-ФЗ

ГОССЕКТОР
Технические средства

Средства ИС госорганов и учреждений размещаются в РФ, зарубежные базы для ГИС исключены, ч.2.1 ст.13 149-ФЗ

2025-2030
КИИ

С 01.01.2025 госорганам и заказчикам по 223-ФЗ запрещено иностранное ПО на значимых объектах КИИ (Указ № 166), переход на доверенные ПАК до 01.01.2030

2027
Модели ИИ

С 01.03.2027 суверенные и национальные модели работают в ЦОД российских юрлиц, 243-ФЗ

ОБСУЖДАЕТСЯ
Облака и ПО бизнеса

Минцифры в 2025 году предлагало запретить крупному бизнесу иностранные облака и ПО в ИСПД с 01.09.2027, нормативно не оформлено

19.2

Практика 2016-2026

Блокировки, штрафы и выводы судов

- динамика штрафов по годам
- ключевые дела и их уроки
- что изменилось в 2026 году

Ретроспектива практики 2016-2026

От блокировки одной сети к потоку дел против иностранных сервисов

Privacy Advocates

2016 **LinkedIn**
реестр нарушителей и ограничение доступа

2018 **Умное голосование**
серверы Cloudflare и метрики как нарушение

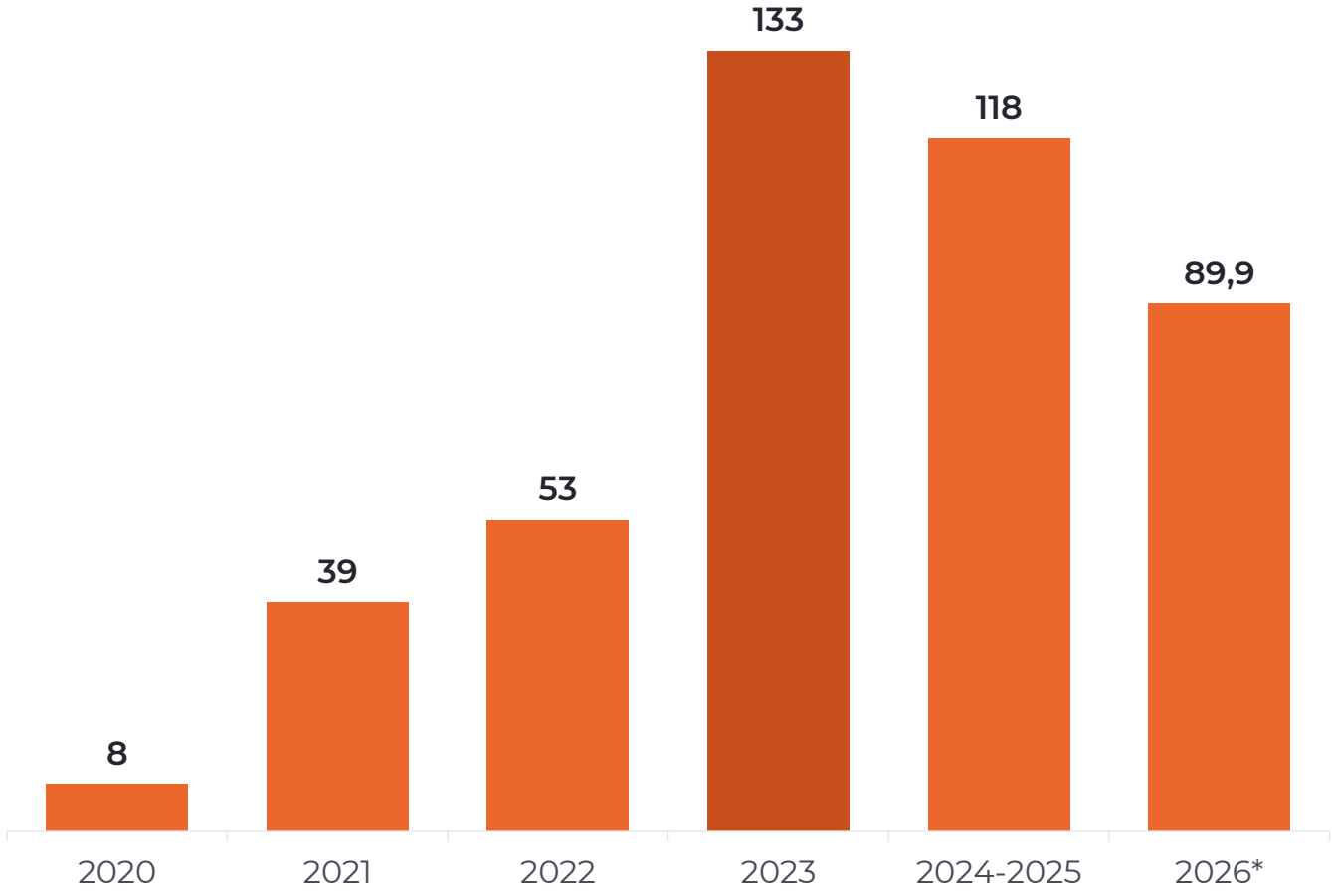
2019 **ВС РФ, Twitter**
непредставление сведений о локализации

2022 **Ookla**
открытой регистрации россиян достаточно

2025 **WhatsApp**
17 млн ₽ за повторное нарушение

2026 **Волна дел**
30+ решений за девять месяцев

Штрафы за нелокализацию, млн ₽



* январь - сентябрь 2026

[2016] Блокировка LinkedIn

Первый и самый известный случай: реестр нарушителей вместо штрафа

Privacy Advocates

04.08.2016
Таганский районный суд удовлетворил иск РКН в защиту неопределенного круга субъектов ПД

10.11.2016
Мосгорсуд оставил решение в силе

17.11.2016
LinkedIn внесен в реестр нарушителей, операторы связи начали блокировку

декабрь 2016
встреча РКН с вице-президентом LinkedIn: требования о локализации разъяснены

07.03.2017
LinkedIn сообщил, что понимания не достигнуто и сервис остается заблокированным

ДОСТУП ИЗ РФ

10 лет

сервис недоступен в России с ноября 2016 года

Направленность на РФ
суд увидел в русскоязычной версии сайта и рекламе на русском языке

Не только серверы
РКН требовал и изменить пользовательское соглашение о передаче ПД третьим лицам

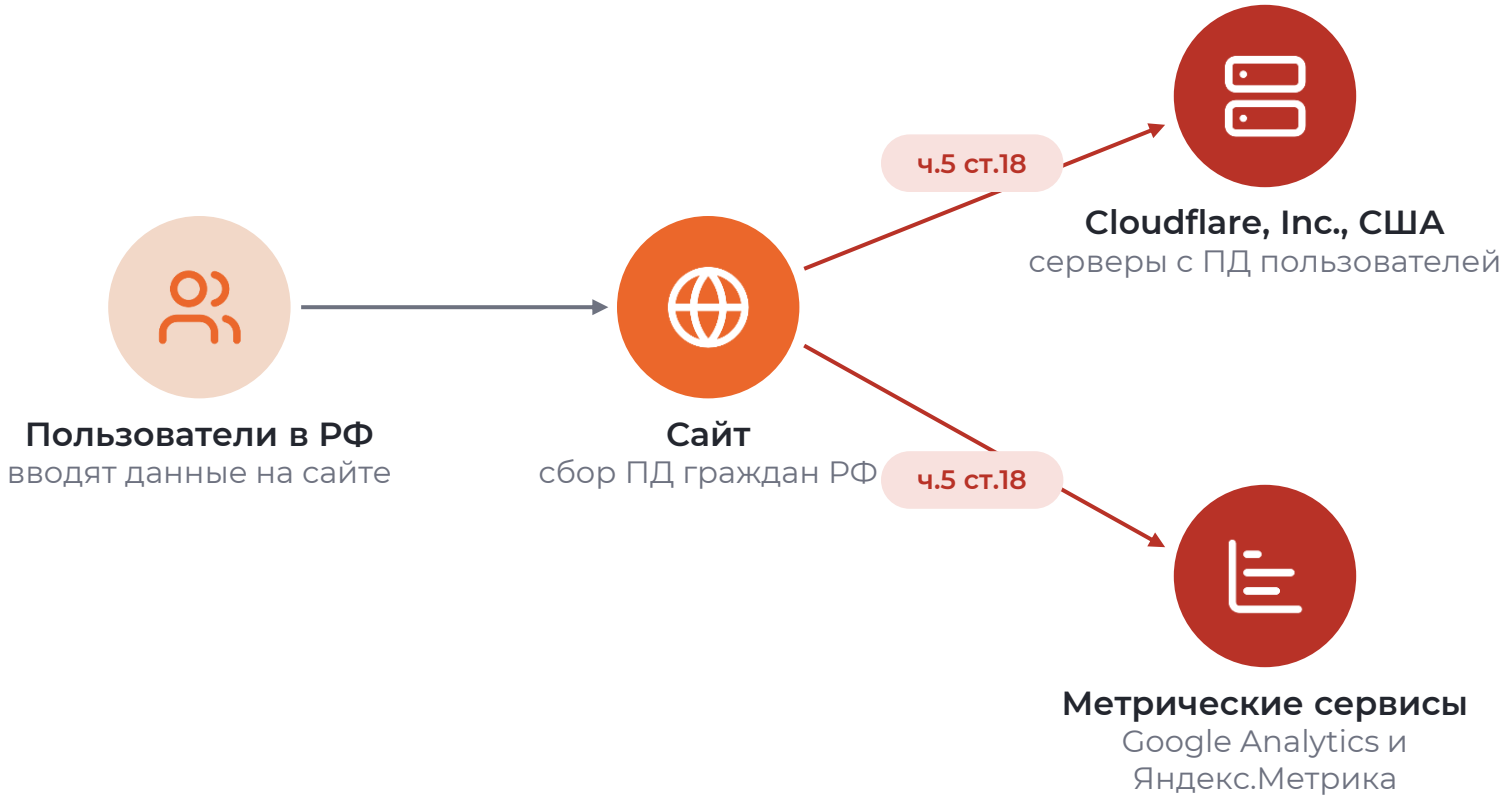
Цена нарушения
для иностранного сервиса риск измеряется потерей российской аудитории, а не штрафом

[2018] Блокировка сайта Умное голосование

Иск РКН удовлетворен Таганским районным судом 19.12.2018, Мосгорсуд оставил решение в силе

Privacy Advocates

ЧТО СУД ПРИЗНАЛ НАРУШЕНИЕМ Ч.5 СТ.18



19.12.2018
Таганский районный суд удовлетворил иск РКН

26.02.2019
Мосгорсуд оставил решение без изменения

ВЫВОД СУДА

Нарушение образуют и хранение ПД пользователей на серверах Cloudflare в США, и использование метрических сервисов, серверы которых, по выводу суда, находятся в США.

Итог - ограничение доступа к ресурсу.

[2020] Штраф 50 тыс. ₽ на должностное лицо

Мировой судья судебного участка № 122 Центрального района Волгограда

Privacy Advocates

Трудовой договор и должностная инструкция → Обязанность подавать сведения в РКН → **Должностное лицо по ст.2.4 КоАП** → Ответственность по ч.8 ст.13.11 КоАП

50 тыс. ₽

вместо 100-200 тыс. ₽ по санкции для должностных лиц: учтены первое привлечение и раскаяние (ч.2.2 ст.4.1 КоАП)

директор Центра немецкого языка ВГСПУ

протокол 23.09.2020, постановление 26.10.2020

ВЫВОДЫ ДЛЯ КОМПАНИЙ

- Ответственный за локализацию работник рискует лично, а не только компания
- Назначение ответственного фиксируют вместе с полномочиями и ресурсами, иначе доказать принятие всех мер сложно
- Санкции для должностных лиц не изменились: по ч.8 100-200 тыс. ₽, повторно по ч.9 500-800 тыс. ₽

[2020] Штраф 8 млн ₽ на Facebook и Twitter

Мировой судья судебного участка № 374 Таганского района Москвы, ч.8 ст.13.11 КоАП

Privacy Advocates

13.02.2020

4 + 4 млн ₽

Twitter и Facebook за отказ перенести базы российских пользователей в РФ

РКН неоднократно направлял компаниям письма с требованием обеспечить хранение данных россиян на серверах в РФ, ответов не было.

ЛЕСТНИЦА ЭСКАЛАЦИИ

02.12.2019

405-ФЗ ввел чч.8 и 9 ст.13.11: юрлица 1-6 млн ₽, повторно 6-18 млн ₽

13.02.2020

первые штрафы по ч.8: по 4 млн ₽ Twitter и Facebook

26.08.2021

повторные штрафы по ч.9: Twitter 17 млн ₽, Facebook 15 млн ₽

[2021] РКН запрашивает адреса серверов

Запрос о локализации стал самостоятельным рычагом надзора

Privacy Advocates

ЗАПРОС РКН О ЛОКАЛИЗАЦИИ

- Заверенная схема размещения серверов с данными российских пользователей
- Договор купли-продажи серверов и справка о постановке их на учет
- При аренде мощностей в российском ЦОД - копия договора аренды
- Сведения о мощностях и договоры с ЦОД (письмо РКН от 14.07.2023 № 08ВМ-59834)

Непредставление сведений - отдельный состав ст.19.7 КоАП

независимо от соблюдения локализации по существу. Так привлекли Twitter в 2019 году, ВС РФ акты оставил в силе.

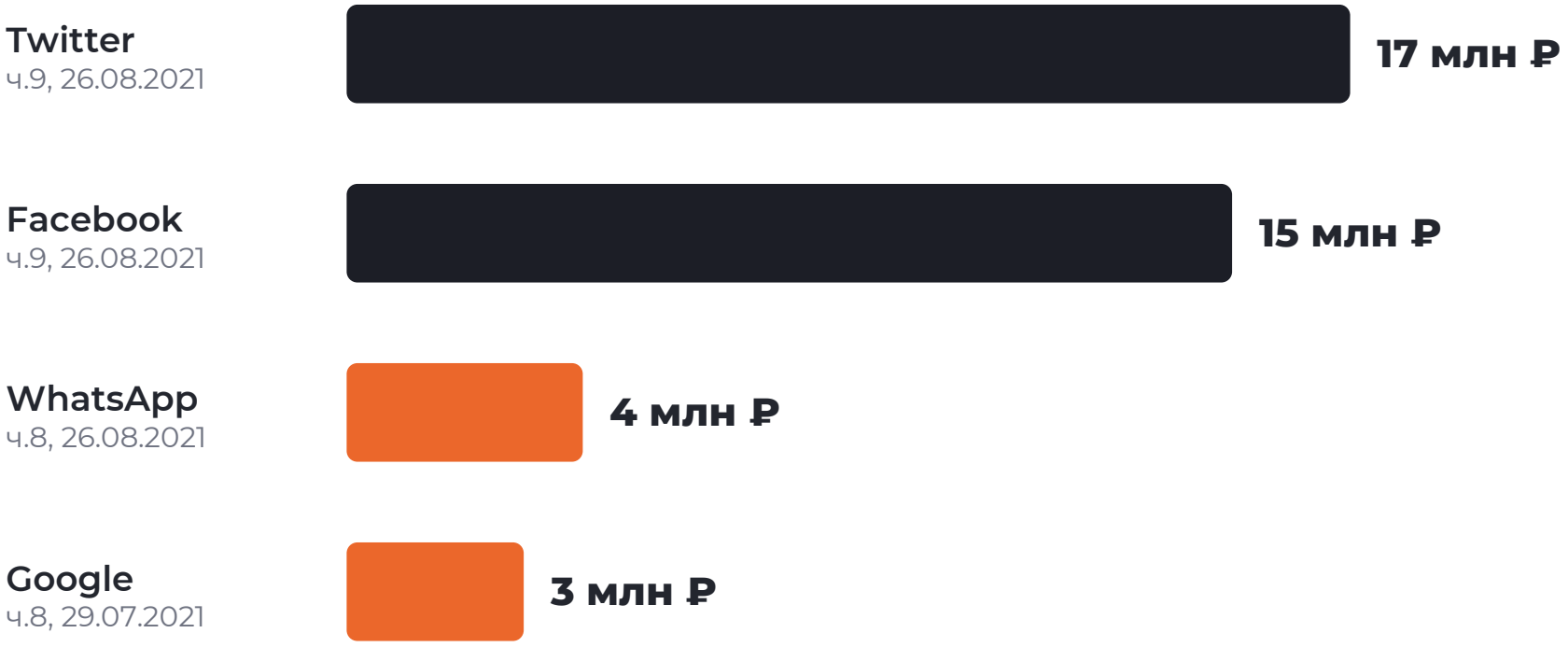
ЧТО ПОДГОТОВИТЬ ЗАРАНЕЕ

- схему размещения баз с ПД граждан РФ
- договоры с ЦОД и документы на оборудование
- политику с указанием места нахождения баз
- журналы, подтверждающие первичную запись в РФ

[2021] Штраф 39 млн ₽ на Google, Facebook, WhatsApp и Twitter

Мировой судья судебного участка № 422 Таганского района Москвы

Privacy Advocates



ЗА 2021 ГОД

39 млн ₽

четыре глобальных сервиса

36 млн ₽ назначено за один день 26.08.2021

Google впервые оштрафован за локализацию

Исполнение: Facebook, Google и WhatsApp выплатили 22 млн ₽ (ТАСС). Twitter и Facebook получили повторные составы ч.9 через полтора года после первых штрафов.

[2022] 53 млн ₽ штрафов

Мировые судьи, в основном судебный участок № 422 Таганского района Москвы

Privacy Advocates

ИТОГО ЗА ПЕРИОД

53 млн ₽

17 решений
по чч.8 и 9 ст.13.11 КоАП

повторно, ч.9: 2

впервые, ч.8: 15

Сохнут: 1 млн ₽, решение Фрунзенского районного суда Санкт-Петербурга от 01.03.2022. Snap: 1 млн ₽ по постановлению от 28.07.2022

WhatsApp
18 млн ₽

Google
15 млн ₽

10 решений по 0,5-1,5 млн ₽
Likee, MyHeritage, Hotels.com, Ookla, Snap (Snapchat), UPS, Zoom, АНО Сохнут, Freelancer.com, Spotify

Airbnb
2 млн ₽

Apple
2 млн ₽

Match Group (Tinder)
2 млн ₽

Pinterest
2 млн ₽

Twitch
2 млн ₽

[2022] Сохнут: 1 млн ₽ за ввод ПД в зарубежную базу

Судебный участок № 181 СПб и Фрунзенский районный суд, решение от 01.03.2022 № 12-228/2022

Privacy Advocates

ЧТО УСТАНОВИЛА ПРОВЕРКА ПРОКУРАТУРЫ С УЧАСТИЕМ РКН



Анкеты и согласия
приходят сканами на почту сотрудника

АРМ сотрудника АНО
ввод ФИО, даты рождения, адреса, паспорта, образования

Ресурс в США
доступ через тонкий клиент по HTTPS, место по whois

ДОВОДЫ ЗАЩИТЫ

- сбор ведет другое лицо, а не АНО
- у АНО есть база на территории РФ
- проверка не исследовала российскую базу

ПОЗИЦИЯ СУДА И ПРОКУРОРА

- сотрудники АНО сами вносили ПД граждан РФ в базу в США
- получение анкет по почте - это сбор
- одновременное хранение в РФ и за рубежом при сборе - нарушение (прокурор)

ИТОГ

1 млн ₽

ч.8 ст.13.11 КоАП, жалоба отклонена 01.03.2022. В июле 2022 года Минюст подал иск о ликвидации представительства, работа с ПД - среди претензий.

Урок: база в РФ не спасает, если сотрудники вносят ПД напрямую в зарубежную систему.

[2022-2023] Выводы из дел о сервисе Speedtest.net

Ookla LLC: 1 млн ₽ по ч.8 в 2022 году, 6 млн ₽ по ч.9 в 2023 году

Privacy Advocates

Направленность не нужна, хватит открытой регистрации

Нет русской версии, политики на русском и расчетов в рублях, но нет и ограничений регистрации россиян, поэтому требование применимо.

Процедуры 248-ФЗ и ПП-336 не защищают

Законодательство о госконтроле к лицу за пределами РФ не применяется.

Сетевые данные - это ПД

Под локализацию попадают сведения о сетевой активности, идентификаторы устройства и cookie, полученные при мониторинге поведения.

Email как уникальный идентификатор

Если для регистрации достаточно адреса почты, который нельзя использовать повторно, он идентифицирует пользователя.

Мера защиты: указание гражданства до доступа плюс ограничение российских IP, подтвержденные скриншотами и журналами

ПОВТОРНОЕ ДЕЛО, 2023

Конкретное нахождение баз данных доказыванию не подлежит

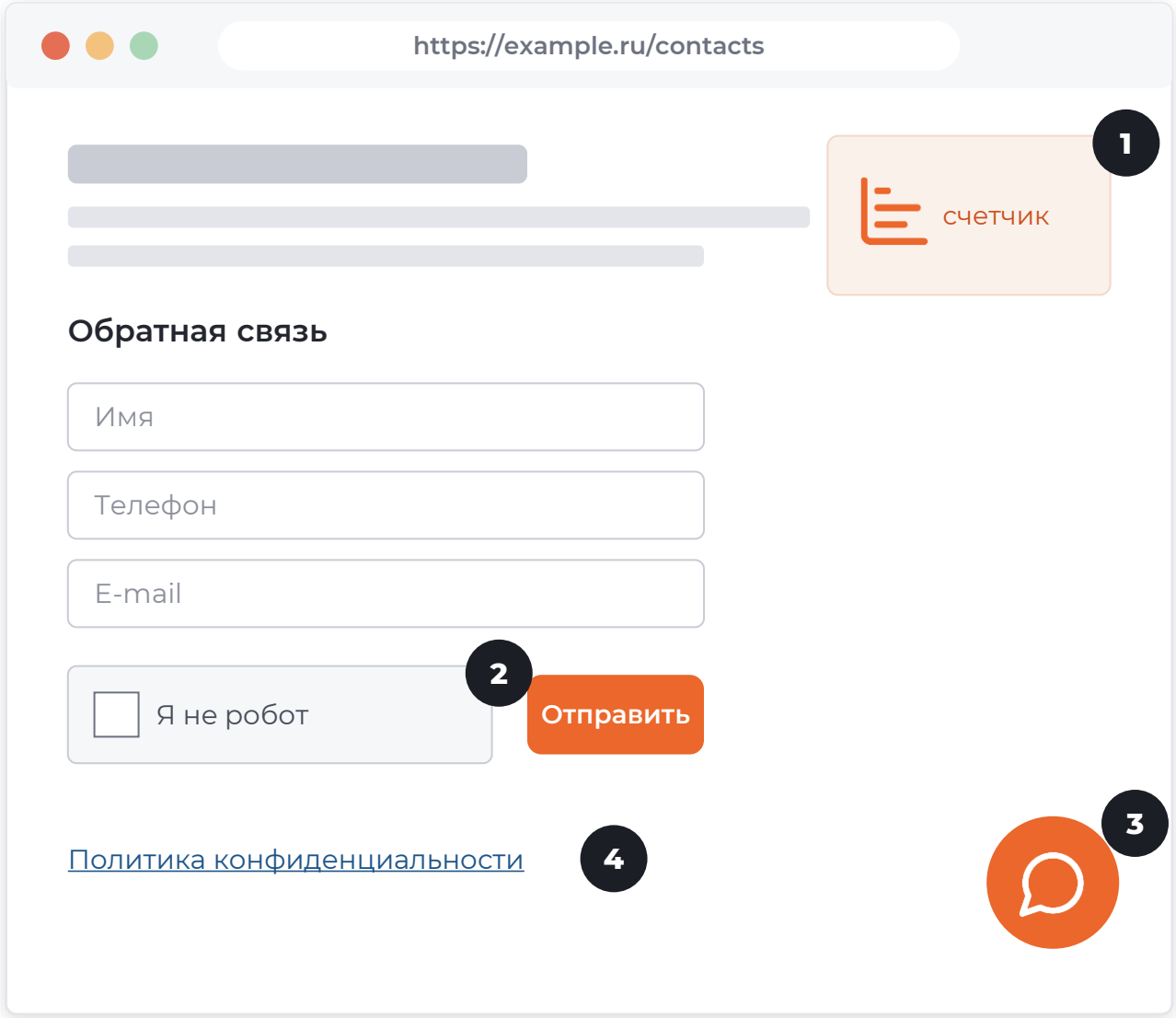
Постановление мирового судьи от 16.10.2023, кассация 14.03.2025 оставила в силе.

На практике бремя доказывания размещения баз смещается на оператора, хотя по ч.3 ст.1.5 КоАП он не обязан доказывать невиновность.

[2022-2023] Иностранные сервисы на сайте - риск

Территориальные управления РКН находят их при внешнем осмотре сайта

Privacy Advocates



1. **Аналитика**
   Google Analytics и аналогичные счетчики передают ПД посетителей на зарубежные серверы

2. **Капча под формой**
   Google-капча под формой обратной связи может указывать на ТПД

3. **Виджеты и внешние формы**
   чаты, формы и кнопки сторонних сервисов собирают ПД в обход базы в РФ

4. **Политика**
   не упоминает ТПД и место нахождения баз

Марий Эл, сентябрь 2022
Управление РКН по ПФО: GA на сайте - нарушение ч.5 ст.18, в том числе ТПД через сервис

Тюмень, сентябрь 2023
5 мероприятий без взаимодействия, нарушения у всех операторов, среди них Google-капча

[2023] 133 млн ₽ штрафов

Повторные составы ч.9 становятся нормой для крупных сервисов

Privacy Advocates

ИТОГО ЗА ПЕРИОД

133 млн ₽

24 решения
по чч.8 и 9 ст.13.11 КоАП

повторно, ч.9: 15

впервые, ч.8: 9

Agoda: штраф заменен предупреждением по ст.4.1.1 КоАП с учетом мер по локализации

12 решений по 0,5-3 млн ₽

Freelancer, UPS, SNSI, SSI International, Padi Americas, AIDA International, Coinbase Ireland, Faceit, International Training, Proxima Beta (PUBG), Molchanovs, Agoda (предупр.)

Google
15 млн ₽

Zoom
15 млн ₽

Twitch
13 млн ₽

Apple
12 млн ₽

Pinterest
12 млн ₽

Snap (Snapchat)
9 млн ₽

Airbnb
6 млн ₽

Match Group (Tinder)
10 млн ₽

Hotels.com
6 млн ₽

MyHeritage
6 млн ₽

Ookla
6 млн ₽

Spotify
6 млн ₽

[2024-2025] 118 млн ₽ штрафов

Крупнейшие суммы - за повторное нарушение

Privacy Advocates

ИТОГО ЗА ПЕРИОД

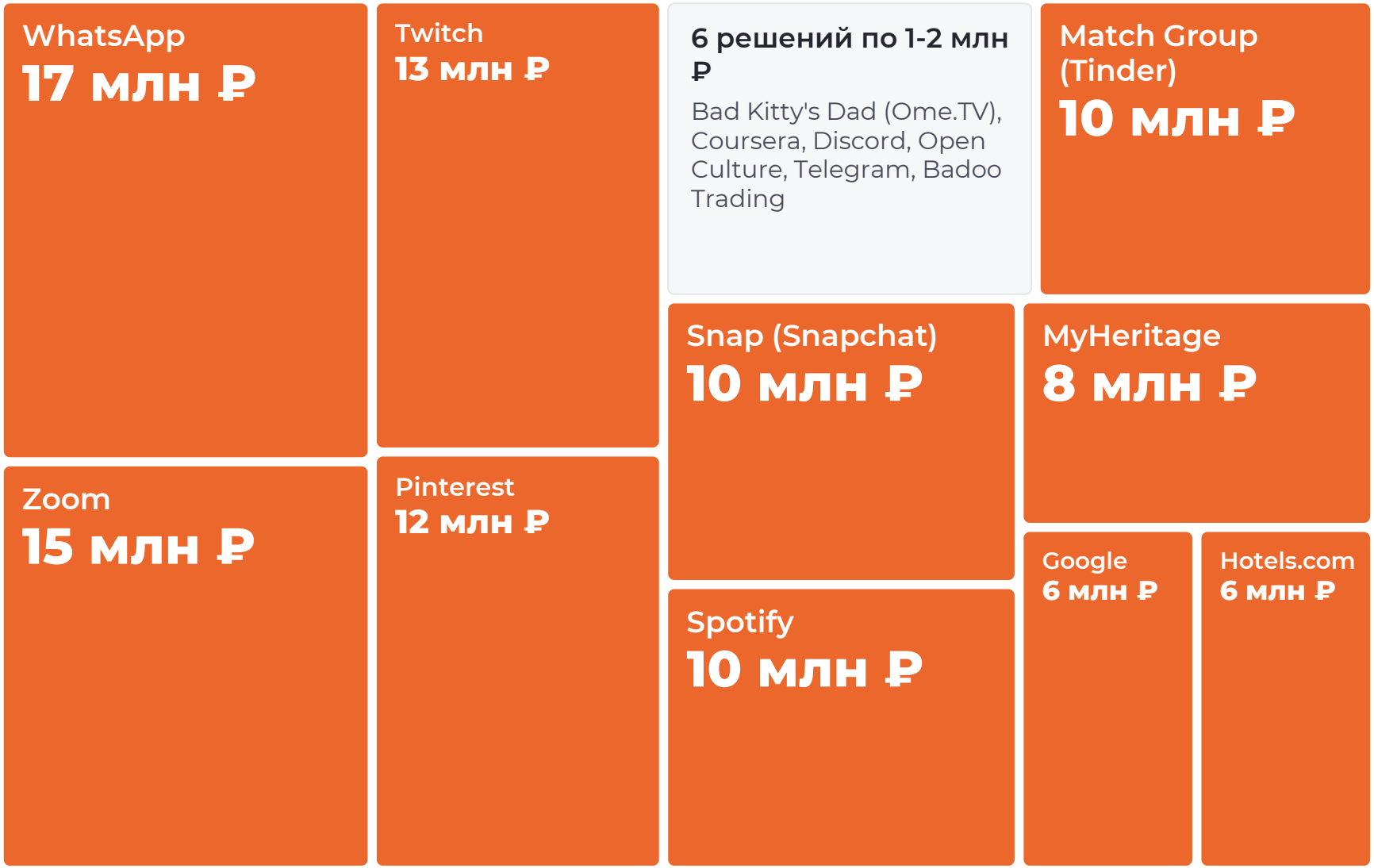
118 млн ₽

16 решений
по чч.8 и 9 ст.13.11 КоАП

повторно, ч.9: 10

впервые, ч.8: 6

Google 6 млн ₽ (17.12.2024), MyHeritage 8 млн ₽ (22.01.2025), Hotels.com 6 млн ₽



[2026] 95,9 млн ₽ штрафов

Январь - сентябрь 2026 года: волна дел против иностранных сервисов

Privacy Advocates

ИТОГО ЗА ПЕРИОД

95,9 млн ₽

33 решения
по чч.8 и 9 ст.13.11 КоАП

повторно, ч.9: 10

впервые, ч.8: 23

По постановлениям судов и сообщениям СМИ. Google 3,8 млн ₽ - 18.08.2026, по данным СМИ

22 решения по 0,1-2 млн ₽

Amo SAS, Battlestate, Duolingo, Electronic Arts, Epic Games, IAB, Miro, NetEase, Realtimeboard Ltd, Take-Two, eNom, Blockchain Tech., Change.org, Digital Extremes, Domains By Proxy, Dynamic Tech., Embracer Group, Italki, Lavalane, Pro New Word, Taobao, ДЛ, Абинский район



[2026] Практика: что изменилось

Волна дел против иностранных сервисов и новые судебные выводы

Privacy Advocates

МАРТ - МАЙ 2026

20+

постановлений одного московского судебного участка по чч.8 и 9 ст.13.11

Тариф стабилен: ч.8 - 1-2 млн ₽, ч.9 - 6 млн ₽. В августе 2026 года Google, по сообщениям СМИ, получил 3,8 млн ₽ по ч.8.

Подсудность

С 2026 года дела по ст.13.11 вернулись в суды общей юрисдикции (508-ФЗ), арбитражные суды дорассматривали принятые ранее.

Планка направленности

Свободный вход из РФ, регистрация с доменом RU и метрика с устройств в РФ - достаточно (Taobao, апелляция 29.09.2026).

Блокировка регистрации

Не защищает, если не закрыты все каналы сбора. Меры доказывает оператор (ч.2 ст.2.1 КоАП).

Место базы

Устанавливают по политике конфиденциальности и whois-сервисам, без технической экспертизы.

Давность

В деле Figma отказано за истечением срока. Дату нарушения суды считают со дня после срока ответа на запрос РКН.

Состав ч.8

Не изменен после 01.07.2025 и описывает неисполнение обязанности обеспечить российские базы.

[2026] Штраф 100 тыс. ₽ на должностное лицо

Мировой судья судебного участка № 113 Абинского района Краснодарского края

Privacy Advocates

1. Заместитель главы администрации Абинского района признана виновной по ч.8 ст.13.11 КоАП
2. Администрация как оператор обрабатывает ПД через интернет-ресурс, в коде страниц которого используется платформа компании из США. Суд квалифицировал это как ТПД в США
3. На платформе размещались сведения об участниках СВО и членах их семей, что, по данным пресс-службы судов, создает угрозу безопасности
4. Уведомление о ТПД в РКН не направлялось, ответственной за это была назначена заместитель главы
5. Доказательств принятия всех зависящих от нее мер суд не получил

КВАЛИФИКАЦИЯ

Фабула - неуведомление о ТПД, а вменена ч.8 (локализация).

Отдельного состава за неуведомление о ТПД нет: в практике встречаются ч.1 и ч.10 ст.13.11, возможна и ст.19.7 КоАП. Сроки давности и санкции при этом несопоставимы.

Урок для сайтов: иностранные скрипты и платформы в коде страниц дают сразу два риска - локализации и неуведомленной ТПД.

19.3

Какие базы локализовать

Какие массивы относятся к первичному контуру сбора

- понятие БД и единый процесс сбора
- сбор против иных способов получения ПД
- экспресс-схема и решения общего назначения
- модель Оператор - Оператор при передаче за рубеж

Определение БД с ПД

В законодательстве несколько понятий БД, для локализации важен упорядоченный массив

Privacy Advocates

ПРИЗНАКИ БД ЧЕРЕЗ Ч.1 СТ.1 152-ФЗ

Носитель

ПД зафиксированы на материальном носителе

Систематизация

картотека или иное собрание ПД

Заданный алгоритм

по нему идут поиск ПД и доступ к ним

Обработка без средств автоматизации подпадает под закон, если по характеру соответствует автоматизированной. Те же признаки отличают БД от разрозненных записей на любом носителе.

СТ.1260 ГК РФ

Совокупность самостоятельных материалов, систематизированных так, чтобы их можно было найти и обработать с помощью ЭВМ

П.2.1 ГОСТ 34.321-96

Совокупность взаимосвязанных данных, организованных по схеме базы данных для работы пользователя

РКН, 09.11.2016

Упорядоченный массив данных независимо от носителя и средств обработки: архивы, картотеки, электронные базы, таблица Excel с ПД

ИСПД ПО П.10 СТ.3 152-ФЗ

ПД в базе данных + **технологии обработки** + **технические средства**

БД - неотъемлемый элемент ИСПД. Дополнительный квалифицирующий признак массива как БД - возможность формально определить его составным элементом ИСПД в РФ.

РКН 22.10.2025 и 14.08.2026: офисные платформы оценивают по определению ИСПД, функционалу конкретного сервиса и потокам данных при его использовании.

Сбор ПД как единый процесс

Момент завершения сбора закон не определяет, его доказывает оператор

Privacy Advocates

ПОЗИЦИИ РКН

09.11.2016: первичное формирование БД на бумаге с последующим внесением в ИСПД - единый процесс.

14.07.2023 № 08ВМ-59834: действия, меняющие состав ПД, сначала выполняются в базах в РФ.

ПОЗИЦИЯ НА ПРИМЕРЕ БЭКАПА

Сбор завершен, когда в базе в РФ сложилась устойчивая запись, пригодная для целей базы

- запись сформирована в базе РФ и годится для целей базы
- с записью начинается рабочая обработка
- параллельно создается бэкап, и первым он тоже хранится в РФ
- только после этого данные передаются за рубеж

Защитимая точка - база в РФ, формально элемент ИСПД в РФ. Кому передавать дальше - на следующем слайде.

СЕМЬ ПРИЗНАКОВ ЗАВЕРШЕННОСТИ СБОРА ПЕРЕД ЭКСПОРТОМ

1. Данные полностью поступили в российскую систему
2. В российской базе есть самостоятельная пригодная запись
3. Достигнута цель российского этапа: заявка, профиль, обращение, кадровое дело
4. Российская база хранит, извлекает и уточняет запись без зарубежной системы
5. Передачу запускает отдельное событие, очередь или регламент
6. Зарубежная система не получает данные из браузера до российской фиксации
7. Последовательность подтверждается журналами

Признаки отделяют сбор от ТПД, но не снимают оценку хранения за рубежом самим оператором (РКН 14.08.2026, устно).

Кому передавать: оператору, а не обработчику

Для локализации модель "Оператор - Оператор" надежнее модели "Оператор - Обработчик"

Privacy Advocates

Оператор (РФ) - Обработчик за рубежом

Оператор
база в РФ

поручение
ч.3 ст.6 152-ФЗ

Обработчик
цели оператора РФ

Данные остаются у того же оператора: копии, снимки и бэкапы за рубежом - зона нарушения ч.5 ст.18

Минцифры 12.05.2025, РКН 14.08.2026 устно

Оператор (РФ) - Оператор за рубежом

Оператор
база в РФ

межоператорское соглашение
ст.12 152-ФЗ

Оператор
собственные цели

Другое лицо получает ранее собранные ПД для своих целей - это ТПД, а не хранение тем же оператором

РКН 24.03.2025, Минцифры 12.05.2025

МЕЖОПЕРАТОРСКОЕ СОГЛАШЕНИЕ: ОБЩАЯ ФОРМУЛИРОВКА ЦЕЛИ, СОБСТВЕННОЕ НАПОЛНЕНИЕ У КАЖДОЙ СТОРОНЫ

Цель в DTA	Для оператора в РФ	Для оператора за рубежом
Управление персоналом	кадровый учет и исполнение трудовых договоров	кадровый резерв и программы вознаграждения группы
Обслуживание клиентов	исполнение договоров с клиентами в РФ	гарантийная поддержка продукта производителем
Отчетность и контроль	бухгалтерская и налоговая отчетность	консолидированная отчетность и аудит группы
ИТ-обеспечение группы	ИТ-поддержка своих систем, основной бэкап базы в РФ	ИТ-услуги и непрерывность группы, бэкап в их составе

Самостоятельность - по факту

- у каждой стороны своя цель и свой интерес в обработке
- получатель сам определяет состав ПД и действия с ними
- без собственной цели получателя квалифицируют как обработчика
- порядок ст.12 сохраняется: основание, сведения, уведомление

Сбор и иные способы получения ПД

Локализация следует за сбором, получение иным способом ее не запускает

Privacy Advocates

Собраны оператором: локализация применима

Предоставленные

получены от субъектов или их представителей

Например: веб-формы, резюме, анкеты

Распространенные

взяты из общедоступных или открытых источников

Например: профили в социальных сетях

Наблюдаемые

зафиксированы путем отслеживания поведения субъектов

Например: онлайн-трекинг, cookie, геолокация

Получены иначе или созданы оператором: локализация не применима

Принятые

получены не от субъектов, а от других лиц

Например: рекомендация прежнего работодателя

Инициированные

образованы действиями в отношении субъектов

Например: выплата зарплаты, трудовой договор

Назначенные

временно или постоянно присвоены субъектам

Например: табельный номер, должность

Производные

синтезированы простым анализом других данных

Например: прибыльность клиента

Предполагаемые

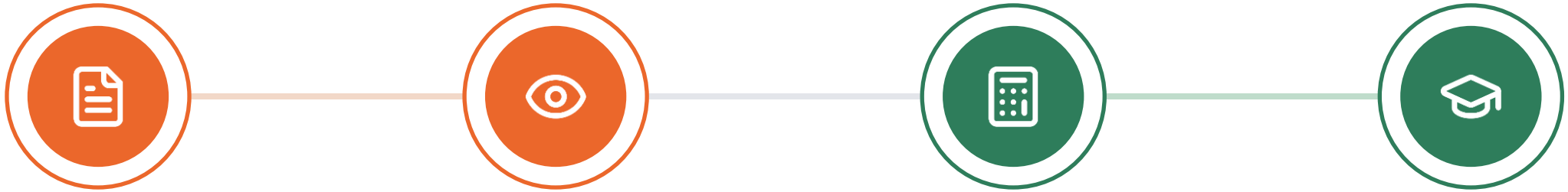
спрогнозированы продвинутым анализом

Например: кредитный рейтинг

Декомпозиция источников ПД на примере онлайн-обучения

Один процесс дает и собранные, и сгенерированные данные

Privacy Advocates



Регистрация через веб-форму

ФИО, e-mail, телефон, дата рождения

Предоставленные

Учет посещаемости занятий

время входа, просмотренные уроки, устройство

Наблюдаемые

Расчет результатов тестирования

баллы, итог теста, рейтинг в группе

Производные

Выдача сертификата

номер и дата сертификата

Назначенные

Сбор ПД

Соблюдаются требования о локализации: первичная запись в базы на территории РФ

Нет сбора ПД

Требования о локализации неприменимы, если хранилище не участвует в записи и уточнении собранных ПД

Экспресс-схема: подлежит ли БД локализации

Четыре вопроса по каждой базе, точность около 95%

Privacy Advocates

1 БД содержит ПД граждан РФ?

нет → **Не подлежит: нет ПД граждан РФ**

да ↓

2 Обработка подпадает под пп.2, 3, 4, 8 ч.1 ст.6 152-ФЗ?

да → **Не подлежит: исключение из ч.5 ст.18**

нет ↓

3 ПД попадают в БД при сборе: от субъектов, из открытых источников, мониторингом поведения?

нет → **Не подлежит: данные сгенерированы или получены иначе**

да ↓

4 Собранные ПД записываются или обновляются напрямую в этой БД?

нет → **Не подлежит: вторичная БД, вывод за рубеж - по правилам ТПД**

да ↓

Подлежит локализации: первичная запись и обновление только в базе в РФ

БД
упорядоченный массив независимо от носителя (РКН 09.11.2016)

Граждане РФ
для иностранного ресурса суды смотрят на доступность из РФ и открытую регистрацию

Копии
зарубежный двойник базы у того же оператора - зона нарушения

Точность
примерно каждая двадцатая БД требует отдельного анализа

Решения общего назначения: двухэтапная проверка

Сначала продукт, затем сценарий его использования

Privacy Advocates

Решение	Может образовать БД	Когда ведется сбор	Вывод
Почта, мессенджеры, ВКС	сообщения и вложения транзитны, схемы данных нет	формы, чат-боты, списки контактов	по потоку
Облачные таблицы и хранилища	файл с упорядоченным массивом - БД (РКН 09.11.2016)	Google-таблицы с ПД граждан - нарушение (РКН 12.01.2026)	исключить
Каталог пользователей, SSO	да, учетные данные ведутся в нем	всегда, он опора для зависимых систем	локализовать
BI и аналитика	да	нет, если загружаются только агрегаты без ПД	не требуется
Метрика, капча, виджеты	данные уходят внешнему сервису	при каждом посещении страницы	российский аналог
Корпоративная почта при запрете сбора	да	нет, если регламент запрещает сбор и он исполняется	документировать

19.4

Стратегии и экономика

Стоимость жизненного цикла против регуляторного риска

- схемы стратегий, затраты и регуляторный риск
- методы оценки расходов и рисков
- калькулятор, ранжирование и дорожная карта

Схемы стратегий локализации

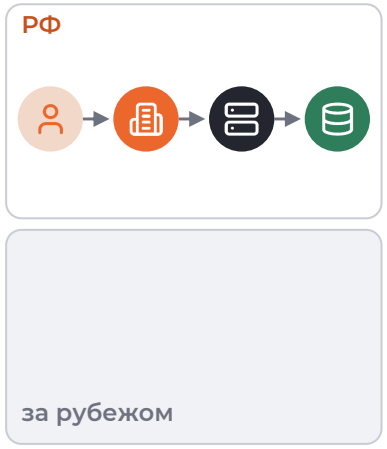
Где оказываются сервер приложений и СУБД при каждой стратегии

Privacy Advocates

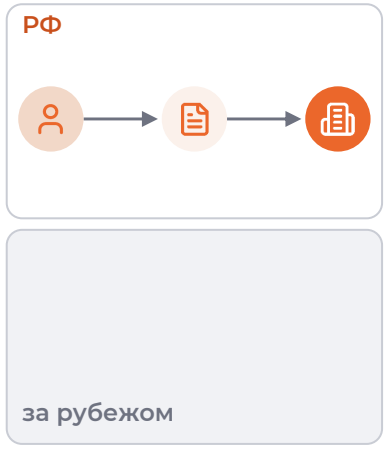
0 Сейчас



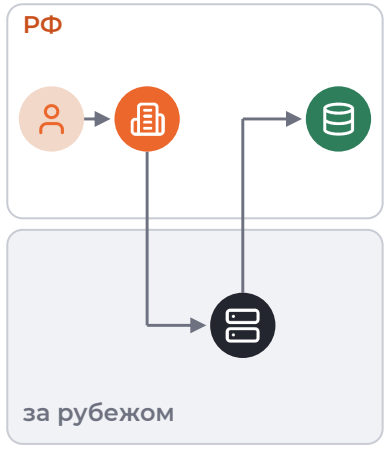
1 Перенос ИСПД в РФ



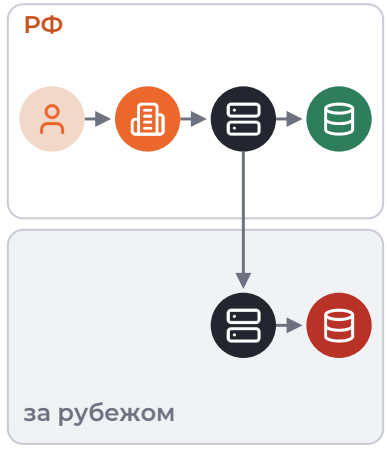
2 Переход на бумагу



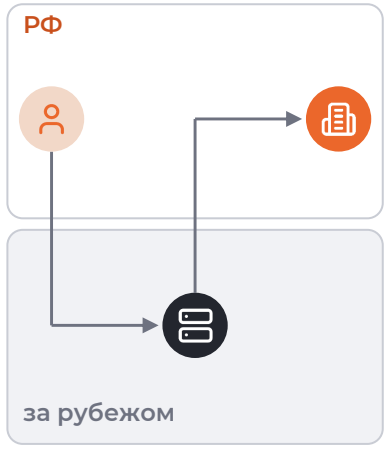
3 Перенос БД в РФ



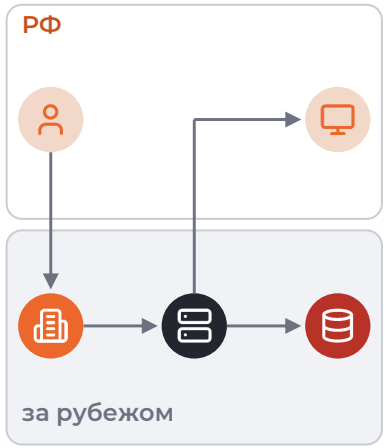
4 Промежуточная БД в РФ



5 Сервис передачи ПД



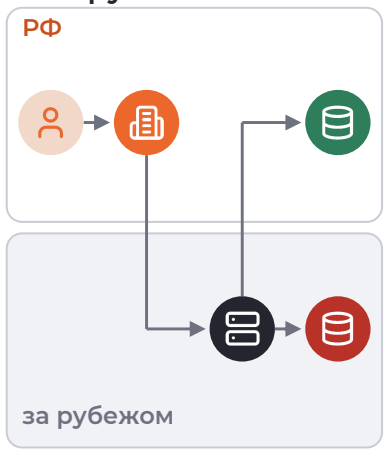
6 Отказ от статуса оператора



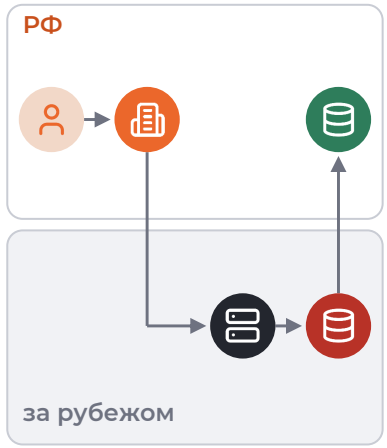
7 Обезличивание или шифрование



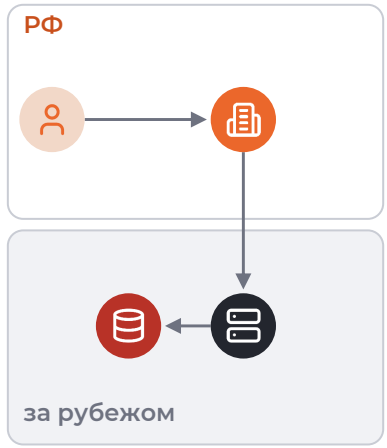
8 Параллельный сбор в РФ и за рубеж



9 Репликация БД в РФ



10 Оставить как есть



- субъект ПД
- оператор
- пользователь
- сервер приложений
- СУБД в РФ
- СУБД за рубежом
- бумага
- обезличивание, шифрование
- цвет номера - риск санкции

Стратегии реагирования на требование локализации

Десять стратегий: затраты и регуляторный риск по калькулятору Privacy Advocates

Privacy Advocates

		затраты, TCO	обнаружение	выявление	суд	публикация	вероятность санкции
1	Перенос ИСПД в РФ	высокий	100%	0%	0%	0%	0%
2	Переход на бумагу	неприменимо	20%	20%	20%	0%	1%
3	Перенос БД в РФ	высокий	100%	20%	20%	20%	4%
4	Промежуточная БД в РФ	низкий	100%	40%	20%	20%	8%
5	Сервис передачи ПД	низкий	80%	40%	40%	20%	13%
6	Отказ от статуса оператора	средний	100%	60%	40%	20%	24%
7	Обезличивание или шифрование	неприменимо	100%	60%	60%	20%	36%
8	Параллельный сбор в РФ и за рубеж	низкий	100%	80%	70%	40%	56%
9	Репликация БД в РФ	средний	100%	80%	80%	40%	64%
10	Оставить как есть	нет	100%	90%	90%	60%	81%

Проценты даны для примера и не являются догмой: вероятности задаются экспертно под каждую ИСПД

Карта стратегий: затраты против риска

Полюса понятны, оптимум для каждой ИСПД лежит между ними

Privacy Advocates



ЛИДЕРЫ КАЛЬКУЛЯТОРА

1. **Стратегия 5** Сервис передачи ПД
2. **Стратегия 4** Промежуточная БД в РФ
3. **Стратегия 6** Отказ от статуса оператора

Решение принимается по каждой ИСПД по сумме стоимости жизненного цикла и совокупного риска, с учетом критичности системы для бизнеса.

Подходы к оценке стоимости стратегий

Количественный расчет и качественная матрица

Privacy Advocates

КОЛИЧЕСТВЕННЫЙ ПРИМЕР, МЛН ₽



КАЧЕСТВЕННЫЙ ПРИМЕР: ВНЕДРЕНИЕ × ПОДДЕРЖКА

затраты на поддержку

	нет	низкий	средний	высокий	очень высокий	н/п
нет	нет	низкий	низкий	средний	высокий	н/п
низкий	низкий	низкий	средний	средний	высокий	н/п
средний	низкий	низкий	средний	высокий	высокий	н/п
высокий	средний	средний	средний	высокий	очень высокий	н/п
очень высокий	средний	высокий	высокий	высокий	очень высокий	н/п
н/п	н/п	н/п	н/п	н/п	н/п	н/п

строки - затраты на внедрение, н/п - неприменимо

Количественный подход точнее, качественный быстрее: для портфеля из десятков ИСПД начинают с матрицы

Оценка расходов на реализацию стратегий

Стоимость жизненного цикла, а не цена внедрения

Privacy Advocates

TCO = CapEx + OpEx × T

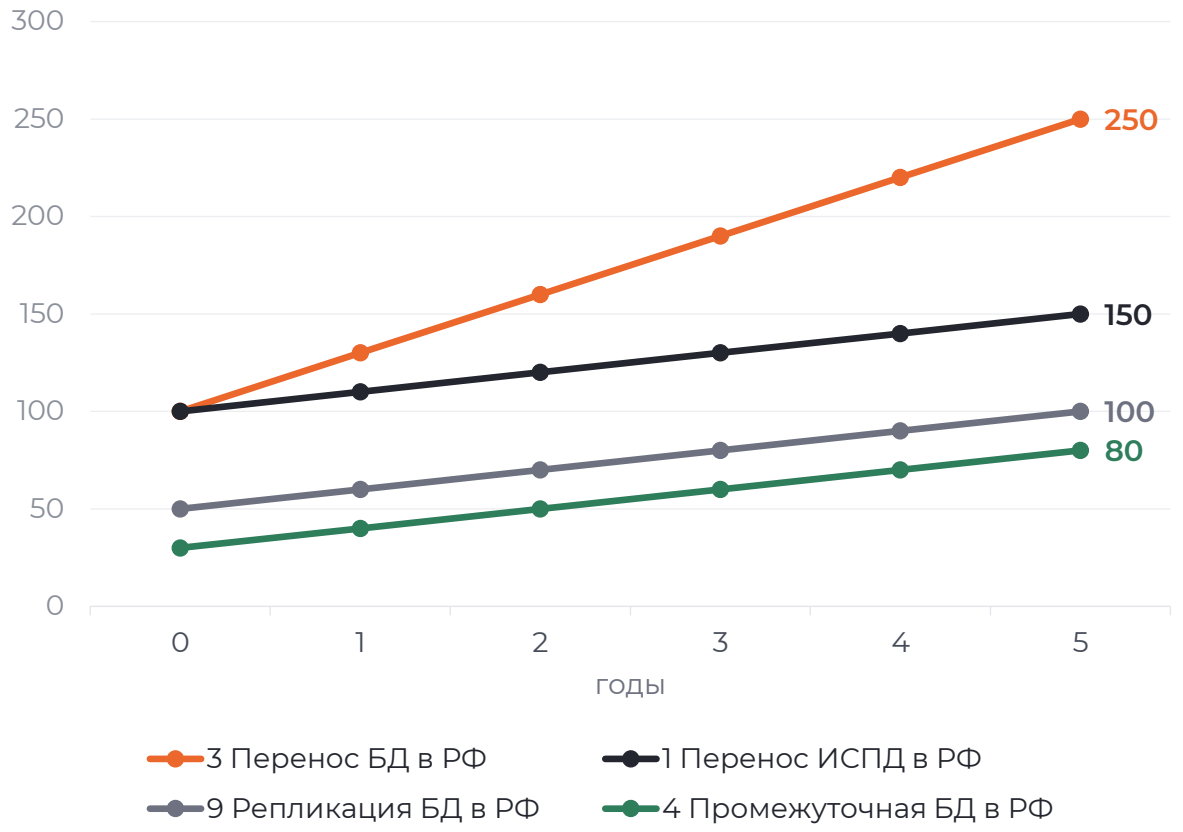
CapEx, однократные расходы
перенос или отделение БД, доработка интеграций и точки первичной записи, миграция каталогов, договоры с ЦОД

OpEx, ежегодные расходы
аренда мощностей в РФ, поддержка, лицензии отечественных замен, сопровождение документов

T, жизненный цикл в годах
горизонт, на котором стратегия остается допустимой с учетом тренда на приземление обработки

Главная статья расходов - трудозатраты на модификацию процесса обработки ПД

НАКОПЛЕННЫЕ ЗАТРАТЫ, БАЛЛЫ КАЛЬКУЛЯТОРА



Одинаковые разовые затраты, разная цена владения: перенос БД в РФ к пятому году обходится на две трети дороже переноса ИСПД целиком

Риски несоблюдения требований о локализации

Штраф - не самое дорогое последствие

Privacy Advocates

Юридические
материальные потери

ч.8 ст.13.11 КоАП
ЮЛ 1-6 млн ₽, ДЛ 100-200 тыс. ₽, граждане 30-50 тыс. ₽

ч.9 ст.13.11 КоАП
повторно: ЮЛ 6-18 млн ₽, ДЛ 500-800 тыс. ₽

ст.19.7 и 19.5 КоАП
непредставление сведений по запросу и невыполнение предписания

Иски субъектов
в том числе групповые по гл.22.3 ГПК РФ

Практические
практический ущерб

Реестр нарушителей
ограничение доступа к ресурсу, ст.15.5 149-ФЗ

Запрет сбора и ТПД
для иностранного лица, ст.16 236-ФЗ

Приостановление обработки
п.4 ч.3 ст.23 152-ФЗ, сжатые сроки, высшая группа тяжести по ПП-1286

Договорные санкции
по соглашениям с контрагентами

Репутационные
репутационный вред

Клиенты и партнеры
утрата лояльности

Инвесторы
недоверие потенциальных контрагентов

СМИ
негативный образ компании и ее должностных лиц

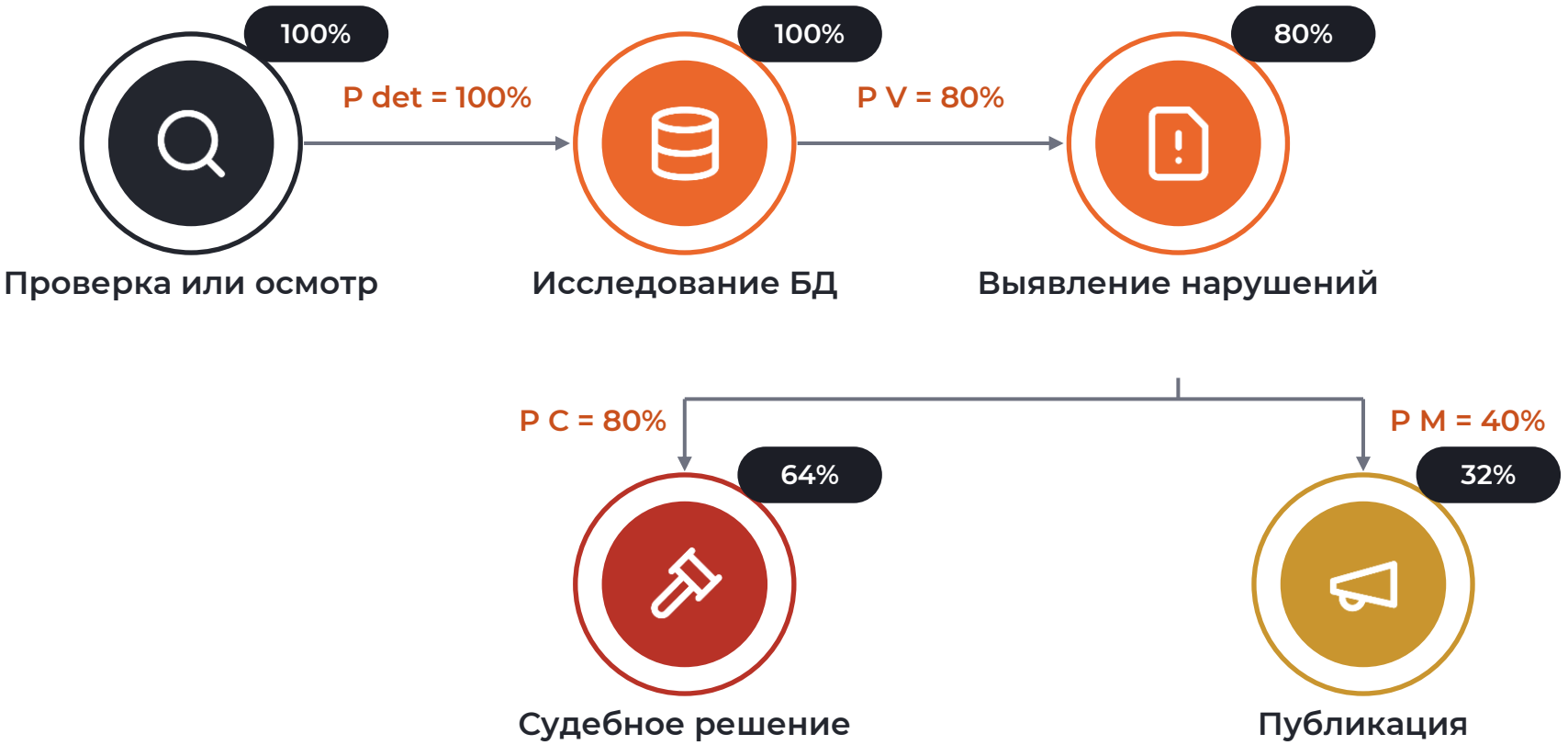
Активисты
атаки privacy-экстремистов

Оборотные штрафы реформы 30.05.2025 касаются повторных утечек, санкции чч.8 и 9 не менялись. Отраслевые требования к хранению проверяются отдельно

Оценка рисков при реализации стратегий

Вероятности звеньев перемножаются: пример для стратегии 9, репликация БД в РФ

Privacy Advocates



РАСЧЕТ СОВОКУПНОГО РИСКА

$1 \times 0{,}8 \times (0{,}8 \times 2 \times 150 + 0{,}4 \times 30)$

= 201,6 балла

M = 2: средняя критичность системы

S1 = 150: затраты на перенос ИСПД целиком

D = 30: средний размер регуляторного риска

Материальные и практические потери
штрафы, иски, перенос БД в сжатые сроки: M × S1

Репутационный вред
клиенты, партнеры, СМИ: D

Факт 2026: место базы устанавливают по политике и whois, P det близка к единице

Формула оценки привлекательности стратегий

Чем меньше S, тем привлекательнее стратегия

Privacy Advocates

$$S_i = C_i + O_i \times T_{lc} + P_{det,i} \times P_{V,i} \times (P_{C,i} \times M \times S_1 + P_{M,i} \times D)$$

стоимость жизненного цикла | совокупный риск

Затраты

- C_i — однократные расходы на стратегию (CapEx)
- O_i — ежегодные расходы (OpEx)
- T_{lc} — жизненный цикл стратегии в годах

Вероятности

- $P_{det,i}$ — обнаружение БД надзорным органом
- $P_{V,i}$ — выявление нарушений в обнаруженной БД
- $P_{C,i}$ — подтверждение нарушения судом
- $P_{M,i}$ — публикация о нарушении

Последствия

- M — мультипликатор влияния на бизнес
- S_1 — затраты на стратегию 1 за жизненный цикл
- D — материальные потери и репутационный вред

Пример, стратегия 4 (промежуточная БД в РФ): S = 30 + 10 × 5 + 1 × 0,4 × (0,2 × 2 × 150 + 0,2 × 30) = 80 + 26,4 = 106,4. Второе место после сервиса передачи ПД (100,3).

Калькулятор оценки стратегий

Оценка одной системы: затраты за жизненный цикл плюс совокупный риск

Калькулятор локализации
скачать

Privacy Advocates

	Внедрение	Поддержка	TCO, 5 лет	Совокупный риск	Место
1 Перенос ИСПД в РФ	очень высокий	низкий	высокий	нет	4
2 Переход на бумагу	н/п	н/п	н/п	низкий	9
3 Перенос БД в РФ	очень высокий	средний	высокий	низкий	7
4 Промежуточная БД в РФ	средний	низкий	низкий	низкий	2
5 Сервис передачи ПД	низкий	низкий	низкий	средний	1
6 Отказ от статуса оператора	высокий	нет	средний	высокий	3
7 Обезличивание или шифрование	н/п	н/п	н/п	очень высокий	10
8 Параллельный сбор в РФ и за рубеж	средний	низкий	низкий	очень высокий	5
9 Репликация БД в РФ	высокий	низкий	средний	очень высокий	8
10 Оставить как есть	нет	нет	нет	очень высокий	6

ШКАЛА ОЦЕНОК

нет = 0	низкий = 10
средний = 30	высокий = 50
очень высокий = 100	н/п = 1000

Параметры примера: жизненный цикл 5 лет, размер регуляторного риска средний (30), мультипликатор влияния на бизнес средний (2).

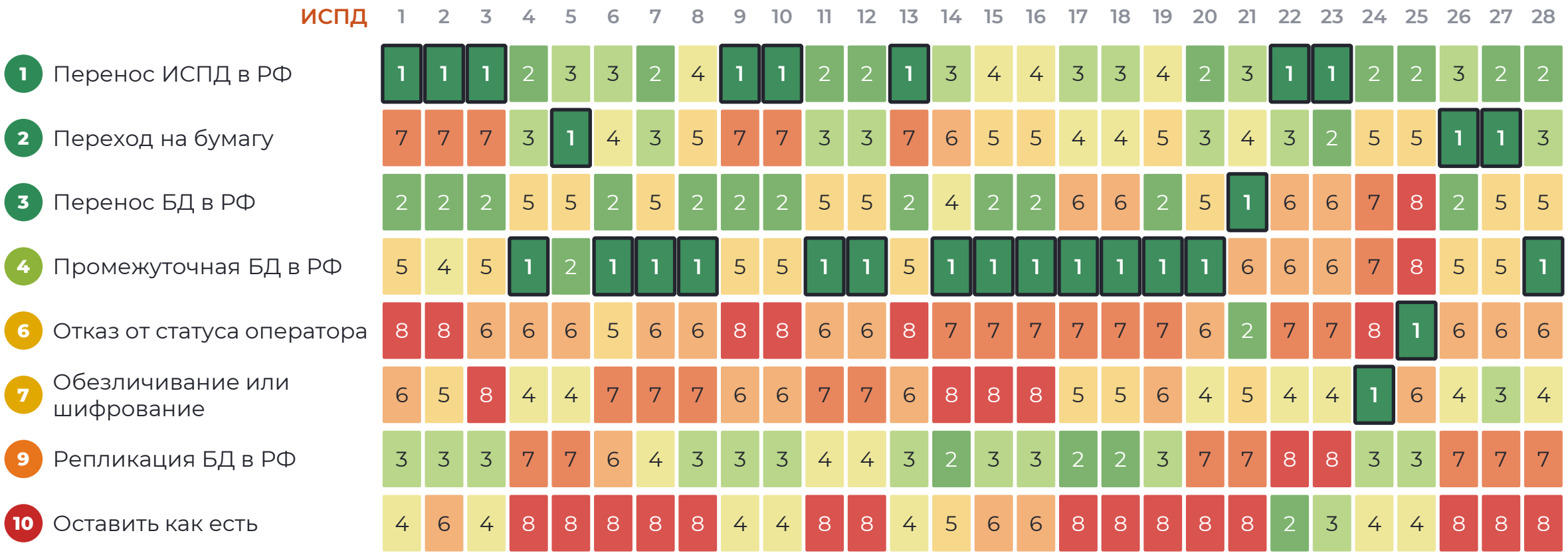
Лидеры: сервис передачи ПД, промежуточная БД в РФ, отказ от статуса оператора. Перенос ИСПД в РФ - четвертый: без риска, но дорого.

н/п - стратегия неприменима

Пример ранжирования стратегий

Портфель из 28 ИСПД: решение принимается по одной таблице

Privacy Advocates



ПЕРВЫЕ МЕСТА

14 из 28 промежуточная БД в РФ

8 перенос ИСПД | **3** бумага | **1** перенос БД | **1** отказ от статуса | **1** обезличивание

Цвет ячейки - место стратегии для системы: 1 зеленый, 8 красный. Рамка - лучшая стратегия.

Проект локализации: шесть шагов

Каждый шаг оставляет документ, который пригодится при проверке

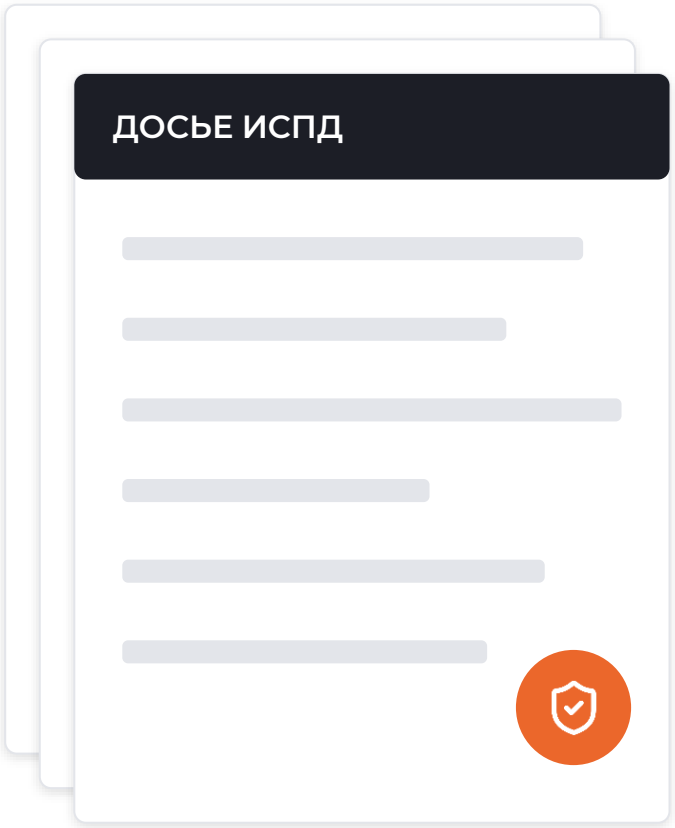
Privacy Advocates

1 Инвентаризация	2 Экспресс-схема	3 Оценка стратегий	4 Решение руководства	5 Внедрение	6 Мониторинг
реестр ИСПД, сервисов, сайтов и потоков ПД граждан РФ	по каждой БД решить, относится ли она к первичному контуру сбора	калькулятор по каждой ИСПД: затраты, вероятности, критичность	выбор по таблице ИСПД и стратегий, принятие остаточного риска	перенос, промежуточные БД, поручения с условием ч.5 ст.18, политика, уведомление РКН	новые сервисы и скрипты, практика и позиции РКН, пересмотр раз в год
реестр ИСПД и карта потоков	**перечень БД первичного контура**	**расчет и ранжирование**	**протокол решения**	**схемы, договоры, уведомление**	**журнал изменений**

Порядок важен: стратегию выбирают после экспресс-схемы, иначе деньги уходят на перенос баз, которые не относятся к первичному контуру сбора.

Доказательства соблюдения локализации

Что держать в досье по каждой ИСПД первичного контура



Инфраструктура

- схема размещения БД и серверов приложений
- договоры с ЦОД, хостингом, облаком в РФ
- документы на оборудование и мощности

Процессы

- описание первичного контура и точки завершения сбора
- журналы первичной записи и обновления
- поручения обработчикам с условием ч.5 ст.18 (ч.3 ст.6)

Публичные документы

- политика с местом нахождения БД
- уведомление РКН с местом нахождения БД (п.10.1 ч.3 ст.22 152-ФЗ)
- описание сервисов и ТПД на сайте

Зачем: суды устанавливают место базы по политике и whois, доказывать меры приходится оператору, а непредставление сведений по запросу РКН - отдельный состав ст.19.7 КоАП.

19.5

Кейс whistleblowing-платформы

- Редакция от 01.04.2022

Горячая линия группы собирает ПД россиян в базу в США

Потоки ПД на whistleblowing-платформе: кто сообщает, где хранится база и кто получает сведения

Privacy Advocates

1 **Заявители в России**

работники и контрагенты ABC, иные заинтересованные лица

2 **Сайт и телефон платформы**

прием сообщений через веб-форму и линию дозвона

3 **База платформы, США**

Platform Provider хранит сообщения как обработчик (data processor)

4 **ABC, Inc., США**

оператор (data controller), получает ПД из базы платформы

5 **Аффилиаты ABC в России**

получатели ПД при эпизодических передачах из США

ПД заявителя

Собраны у самого заявителя

- сбор у субъекта запускает требование локализации
- запись и хранение ПД граждан РФ при сборе в базе в США с 01.07.2025 прямо не допускаются

vs

ПД иных лиц

Получены от заявителя о других людях

- по экспертному подходу данные от третьего лица сбора не образуют
- но Роскомнадзор (22.01.2026) считает сбором и получение ПД от иного лица, поэтому вывод спорен

Риск: если оператор - российский аффилиат, а платформа собирает сообщения в его интересах, локализация остается на нем: чьей цели служит сбор, тот и локализует

Риск горячей линии снижают сменой оператора и анонимностью

Два уровня мер для whistleblowing-платформы и их оценка по редакции ч.5 ст.18 с 01.07.2025

Privacy Advocates

Базовый уровень

Отказ российских компаний от статуса оператора

- признать ABC, Inc. (США) оператором ПД на платформе
- опубликовать Privacy Notice: оператор ABC, Inc., аффилиаты в РФ - получатели ПД
- заключить между ними соглашение о передаче ПД без поручения (DTA)

+

Дополнительный уровень

Анонимность заявителей

- оставить только опцию анонимного сообщения
- рекомендовать не раскрывать личность и контакты
- дать локализованные в РФ каналы тем, кто называет себя

ОЦЕНКА 2026

Обе стратегии - с высоким риском

по каталогу стратегий передача статуса оператора иностранному лицу и обезличивание при сборе стоят дешево, но несут высокий регуляторный риск

Иностранный оператор

статус из режима не выводит: в 2026 году иностранным операторам назначены штрафы по чч.8 и 9 ст.13.11 КоАП

Анонимность

сообщение о других людях остается ПД, а обезличенные данные, по устным позициям Роскомнадзора 2025 года, локализуются

Запрещено с 01.07.2025

параллельный сбор в российскую и зарубежную базы и репликация из зарубежной в российскую

КЛЮЧЕВЫЕ ВЫВОДЫ

- Локализуется первичный контур сбора: запись и обновление ПД граждан РФ идут в базах в РФ, ТПД ранее собранных ПД возможна по ст.12.
- Зарубежные копии, реплики и бэкапы собранных ПД у того же оператора - зона нарушения по позициям Минцифры (2025) и РКН (2025-2026).
- Практика 2026 года: поток дел, ч.8 - 1-2 млн ₽, ч.9 - 6 млн ₽, планка направленности снизилась до доступности ресурса.
- Стратегию выбирают по каждой ИСПД по стоимости жизненного цикла и совокупному риску, с запасом под приземление обработки.

20

Трансграничная передача ПД

Порядок, оценка получателя и практика 2023-2026

20.1 Понятие и регулирование ТПД

20.2 Порядок ТПД и оценка получателя

20.3 Уведомление о намерении

20.4 Практика и ответственность

20.5 Практикум

Раздел на сайте
privacy-advocates.ru/pd/tpd

РАЗДЕЛ 20. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПД

20.1

Понятие и регулирование ТПД

Что считается передачей и как ее читают регуляторы

- общий и секторальные режимы
- примеры наличия и отсутствия ТПД, спорные зоны
- позиции РКН и Минцифры 2022-2026
- российский режим среди мировых моделей

Регулирование ТПД в РФ

Общий режим ст.12 152-ФЗ и секторальные правила, которые проверяются первыми

Privacy Advocates

ОБЩИЙ РЕЖИМ

ст.12 152-ФЗ

1. **Основание и цель**
   из ч.1 ст.6, цель как фактическая деятельность
2. **Оценка получателя**
   сведения по ч.5 ст.12 до подачи уведомления
3. **Уведомление о намерении**
   чч.3-4 ст.12, отдельно от уведомления об обработке
4. **Решения РКН**
   запрет или ограничение по чч.7-12 ст.12

п.11 ст.3: ТПД - передача ПД на территорию иностранного государства иностранному органу власти, физическому или юридическому лицу

СЕКТОРАЛЬНЫЕ РЕЖИМЫ

572-ФЗ, ч.21 ст.3
запрет идентификации и аутентификации с ТПД биометрии, кроме аутентификации госорганами и ЦБ РФ

86-ФЗ, ст.13.1, 13.2, ПП-750
генетические данные с 01.09.2026: свободный, уведомительный и разрешительный маршруты

87-ФЗ, п.11 ст.4
ПД клиентов экспедитора за рубеж не передаются, кроме международных перевозок

ПП-2526 от 29.12.2022
16 публично-правовых случаев без уведомления, еще 4 - уведомление без права запрета

236-ФЗ, ст.16
иностранному лицу-нарушителю в интернете РКН может запретить сбор и ТПД ПД граждан РФ

ст.272.1 УК, ч.4
ТПД и трансграничное перемещение носителей - квалифицирующие признаки

Понятие ТПД

Три условия выполняются одновременно, п.11 ст.3 152-ФЗ

Privacy Advocates

Передача

предоставление или доступ к ПД

+

Из РФ

на территорию иностранного государства

+

Иностранному лицу

органу власти, физическому или юридическому лицу

=

ТПД

Целенаправленность

экспертный признак: передачу инициирует оператор, а не пользователь сайта или сам субъект

Оператор и оператор

РКН 14.08.2026: ТПД складывается в отношениях оператора с оператором

Суть режима

смена юрисдикции над данными: страна регистрации получателя и страна серверов учитываются вместе (РКН 14.08.2026)

Граница и носители

с 2011 года пересечение границы не признак ТПД (261-ФЗ), но перемещение носителей стало признаком ст.272.1 УК

Нет хотя бы одного условия - нет ТПД, но вопрос локализации по ч.5 ст.18 может остаться.

Примеры наличия ТПД

Типовые сценарии, для которых нужны основание, оценка получателя и уведомление

Privacy Advocates

Корпоративная группа

- отчетность с ПД для иностранной материнской компании и ее контрагентов
- участие материнской компании, аудиторов и юрфирм в аудите и расследованиях
- ПД персонала в глобальном справочнике, портале, Active Directory
- ПД, которые российский филиал передает своей иностранной компании

Облака и сервисы

- зарубежные облака для обработки и бэкапа: Azure, Google Cloud, AWS
- специализированные платформы: Google Analytics, SAP, Workday, Salesforce
- ПД провайдерам облаков, почты, ВКС и мессенджеров для служебных учетных записей

Работники и поездки

- бронирование зарубежных гостиниц и билетов у иностранных компаний
- участие лиц из РФ в зарубежных мероприятиях
- открытие счетов и оформление полисов за рубежом

Переписка и доступ

- контакты персонала зарубежным получателям в деловой и договорной работе
- доступ находящихся за рубежом иностранных лиц, например персонала подрядчика, к ПД в РФ

Примеры отсутствия ТПД

Нет иностранного получателя, нет маршрута из РФ или нет целенаправленной передачи

Privacy Advocates

Получатель не иностранный

- представительство или филиал иностранной компании, зарегистрированные в РФ
- гражданин РФ за рубежом, в том числе работник, и его доступ к ПД в РФ
- зарубежный филиал российской компании без статуса юрлица (спорно)

Маршрут не из РФ

- транзит через иностранную территорию между лицами и системами в РФ
- передача из иностранного государства в РФ и между иностранными государствами
- возврат данных от иностранного обработчика оператору в РФ

Нет целенаправленной передачи

- распространение неопределенному кругу лиц
- передача ПД за рубеж самим субъектом
- канал в иностранном мессенджере для пользователей из РФ
- сервисы без обработки ПД, например Google Tag Manager

Офисные облака, почта, ВКС

- целевое использование, например переписка и ВКС двух компаний в РФ, - вряд ли ТПД
- но служебные учетные записи у иностранного провайдера могут быть ТПД (Microsoft 365, Google Workspace, Zoom)
- хранение там ПД граждан РФ нарушает локализацию (РКН 26.09.2025, 12.01.2026)

Спорные зоны квалификации

Позиции расходятся, при сомнениях безопаснее более строгая

Privacy Advocates

НЕ ТПД — *куда склоняются позиции регуляторов* — ТПД

Зарубежный филиал российского юрлица

филиал не иностранное лицо (РКН устно 29.09.2022, 01.03.2023, 27.08.2025)

передача филиалу в другой стране - ТПД (РКН устно 15.05.2024)

Офисные облака и почта

использование сервисов компаниями в РФ - не ТПД, сервисы Google - не ТПД (Управление РКН, 26.09.2025)

служебные учетные записи у иностранного провайдера, облака для обработки и бэкапа - ТПД

Переписка при оценке получателя

сопутствующая передача ради исполнения ст.12 отдельно не уведомляется

контакты работника в переписке - ТПД с уведомлением (РКН 01.06.2023, Минцифры 07.04.2023)

Служебные данные сотрудника

минимальный набор без возможности идентификации - не ПД и не ТПД (Управление РКН по СКФО, 2026)

идентифицирующий объем требует уведомления

Рекомендация: при споре о квалификации выбирать более строгую позицию и включать поток в уведомление.

По экспертному подходу доступ гражданина РФ из-за рубежа не ТПД

Получатель с гражданством РФ, иностранец и апатрид: кто из них иностранное лицо по п.11 ст.3 152-ФЗ

Privacy Advocates

КТО ПОЛУЧАЕТ ДОСТУП ИЗ-ЗА РУБЕЖА	ТПД	ПОЧЕМУ
гражданин РФ, в том числе с иным гражданством	нет	для РФ он только ее гражданин вне зависимости от места проживания (ч.1 ст.10 138-ФЗ), разъяснений РКН нет
он же получает данные для иностранной компании	да	по экспертному подходу получатель - иностранное юрлицо
иностранный гражданин	да	иностранное физическое лицо на территории иностранного государства
лицо без гражданства	спорно	не гражданин РФ (ст.2 115-ФЗ), в режиме ПД приравнен к иностранцу, страну оценивают по месту нахождения
любой из них, пока находится в России	нет	нет территории иностранного государства (РКН устно 22.10.2025)

ЭКСПЕРТНЫЙ ПОДХОД

Что проверить перед доступом

- гражданство РФ подтверждают документом и фиксируют в реестре доступа, иначе получателя считают иностранцем
- исключения из ч.1 ст.10 138-ФЗ дают федеральный закон или международный договор
- иностранное облако с данными дает ТПД провайдеру, мессенджер к гражданину РФ ее не дает (РКН устно 14.08.2026)
- доступ идет к базам в РФ, локализация по ч.5 ст.18 не отменяется

Не путать: гражданство субъекта, чьи данные передаются, квалификацию не меняет (РКН устно 15.05.2024, 22.10.2025). Решают территория и статус получателя

По экспертному подходу выдача иностранцу его собственных ПД не ТПД

Российский оператор и иностранный субъект за рубежом: буква п.11 ст.3 и логика отношений операторов

Privacy Advocates

Буква закона

Похоже на ТПД

- п.11 ст.3 называет получателем и иностранное физическое лицо, оговорки о самом субъекте нет
- гражданство субъекта квалификацию не меняет (РКН устно 15.05.2024, 22.10.2025)
- буквально уведомление нужно до первого ответа иностранцу на запрос по ст.14

vs

Логика режима

Не ТПД по экспертному подходу

- ТПД складывается в отношениях оператора с оператором (РКН устно 14.08.2026)
- субъект со своими данными для личных нужд оператором не становится (п.1 ч.2 ст.1 152-ФЗ)
- выдача сведений исполняет права субъекта по ст.14 и 20, а ст.12 его защищает, а не отрезает от данных

ГДЕ ВЫВОД ПЕРЕСТАЕТ РАБОТАТЬ (ЭКСПЕРТНЫЙ ПОДХОД)

Чужие данные
в пакете ПД попутчиков, родных или созаемщиков: для них это ТПД

Не сам субъект
представитель, работодатель или банк за рубежом - иностранное лицо

Канал оператора
иностранные облако, CRM или почта, где оператор хранит данные, дают ТПД провайдеру

Перенос по просьбе
данные субъекта по его просьбе для зарубежной компании - это ТПД

Практика: прямых разъяснений нет. Включать ли поток в уведомление, решают осознанно и фиксируют в реестре, ведь описание деятельности вне ТПД Роскомнадзор устно (27.08.2025) считает ошибкой

Локализация и ТПД: два независимых контура

Каждый поток данных за рубеж проверяется по обоим

Privacy Advocates

Соблюдение локализации не легализует ТПД, а законная ТПД не исцеляет нарушение локализации

ШАГ 1

Первая запись ПД граждан РФ при сборе происходит в зарубежной системе?

да → **нарушение ч.5 ст.18**

нет →

ШАГ 2

Зарубежная система ведет актуализируемую копию российской базы?

да → **нарушение ч.5 ст.18**

нет →

ШАГ 3

За рубеж уходит выгрузка части ПД под конкретную цель?

да → **это ТПД, далее шаг 4**

нет →

ШАГ 4

Соблюден порядок ТПД: основание, оценка получателя, уведомление?

да → **поток правомерен**

Исключения: пп.2, 3, 4, 8 ч.1 ст.6 снимают требование локализации, но не порядок ТПД. Офисные облака и Google-таблицы по позиции РКН 2025-2026 - вопрос локализации, а не ТПД.

Позиции регуляторов 2022-2024

Письма РКН и Минцифры, которые определили практику нового порядка

Privacy Advocates

09.11.2022 РКН, 08ВМ-98928 — порядок

переходные уведомления об осуществлении ТПД, после 01.03.2023 - о намерении

06.12.2022 РКН, 08ВМ-107716 — порядок

оценка по ч.5 - компетенция оператора, уведомление не по каждому факту и контрагенту

15.02.2023 РКН, 08-12444 — порядок

ТПД до реформы - уведомить до 01.03.2023 независимо от поручения

15.02.2023 РКН, ответ на 02-11-4435 — ТПД

в уведомлении указывается государство серверов иностранного лица

27.03.2023 РКН, ответ на 02-11-9606 — ТПД

доступ иностранных лиц к корпоративному справочнику - ТПД

07.04.2023 Минцифры, П25-7258-ОГ — ТПД

контакты работника в переписке на иностранный почтовый сервер - ТПД

01.06.2023 РКН, 08-46101 — ТПД

контакты в деловой переписке - ТПД, нужно уведомление

14.12.2023 РКН, 08-145976 — не ТПД

канал в Telegram со входом по ссылке-приглашению - не ТПД

18.04.2024 РКН, 08-119857 — порядок

новое уведомление - только при новых потоках: цели или страны

26.06.2024 РКН, 08-242780 — ТПД

Google Analytics на сайте - ТПД, требуется уведомление

Позиции регуляторов 2025-2026

Метрики, облака и мессенджеры: граница между ТПД и локализацией

Privacy Advocates

24.03.2025 РКН, 08-134789 и 08-169079 — порядок

ч.5 ст.18 не ограничивает ТПД ранее собранных в РФ ПД, ст.12 сохраняется

12.05.2025 Минцифры, П25-44929 — ТПД

зарубежные метрические программы - ТПД, копии ведутся в РФ

03.07.2025 Минцифры — не ТПД

сообщения через иностранный мессенджер пользователям в РФ - не ТПД

16.07.2025 Управление РКН по ЦФО — порядок

перечень стран формируется по критериям Конвенции 108

04.08.2025 РКН, 08-373883 — ТПД

зарубежные метрики - ТПД, допустима при соблюдении ч.5 ст.18

19.08.2025 Управление РКН по ПФО — не ТПД

Telegram не обработчик, сообщения в канале - не ТПД

26.09.2025 Управление РКН по Пермскому краю — не ТПД

сервисы Google - не ТПД, но нужна локализация

01.11.2025 РКН, ответ — не ТПД

Google-таблицы с ранее собранными ПД - не ТПД, уведомление не рассматривается

2026 Управление РКН по СКФО — не ТПД

служебные данные без идентификации - не ТПД

14.08.2026 РКН, день открытых дверей — порядок

оператор с оператором, страна регистрации и серверов вместе, запрет по любой стране

Эволюция регулирования ТПД

От письменного согласия к уведомлению и оценке получателя

Privacy Advocates

25.07.2011
261-ФЗ
из определения исключено пересечение границы

14.07.2022
266-ФЗ
новый порядок ТПД, старт с 01.03.2023

05.08.2022
Приказ РКН № 128
перечень адекватных стран

29.12.2022
ПП-2526
случаи без уведомления

10.01.2023
ПП-6
решения по представлениям ведомств

16.01.2023
ПП-24
решения РКН по уведомлениям

01.03.2023
Старт
уведомления о намерении

26.07.2026
265-ФЗ
адекватность только по перечню РКН

16.09.2026
Приказ РКН № 253
88 стран, с 30.10.2026

До 01.03.2023: в неадекватные страны - по письменному согласию субъекта, без уведомления РКН

С 01.03.2023: основание по ч.1 ст.6, оценка получателя и уведомление о намерении до начала передачи

Российский режим ТПД среди мировых моделей

Срединное положение между договорной логикой ЕС и административной логикой Китая

Privacy Advocates

	ЕС, GDPR	Россия, 152-ФЗ	Китай, PIPL
	договорные гарантии		*административное согласование*
Адекватность	решение Еврокомиссии, передача приравнена к внутренней	перечень РКН, но сведения о получателе и уведомление нужны для любой страны	института адекватности нет
Гарантии	SCC, BCR, кодексы и сертификация (ст.46-47 GDPR)	SCC и BCR закон не знает, их заменяют перечень, оценка получателя и уведомление	типовой договор и сертификация
Регулятор	разрешение лишь для части гарантий, после Schrems II - оценка воздействия передачи	уведомление о намерении до передачи, запрет или ограничение решением РКН	оценка безопасности регулятора для КИИ и операторов выше порога (ст.40 PIPL)
Локализация	общего требования нет	первичный сбор ПД граждан РФ в базы в РФ (ч.5 ст.18)	для КИИ и крупных операторов данных

Практический вывод: европейские инструменты в российском контуре напрямую не работают, а при обратной передаче из ЕС от российской компании ждут SCC и оценки воздействия.

20.2

Порядок ТПД и оценка получателя

Категория страны, сведения от получателя и риски запрета

- перечень стран и 265-ФЗ
- порядок, сроки и сведения по ч.5 ст.12
- риски, запрет и ограничение

Не все юрисдикции одинаково полезны

Категория по перечню РКН и дружественность - разные оси

Privacy Advocates

	в перечне РКН: старт после уведомления	вне перечня: старт после 10 рабочих дней
дружественные	**В перечне, дружественные** ЕАЭС, Азербайджан, Сербия, Аргентина, Бразилия, Мексика, Малайзия, Китай, Индия, Вьетнам, ЮАР, Сингапур, Израиль, Турция, Катар	**Вне перечня, дружественные** ОАЭ, Бахрейн, Иран, Боливия, Венесуэла, Египет, Филиппины, Гонконг (Китай)
недружественные (430-р)	**В перечне, недружественные** ЕС, Великобритания, Швейцария, Норвегия, Австралия, Новая Зеландия, Канада, Япония, Южная Корея	**Вне перечня, недружественные** США, Тайвань (Китай)

Примеры стран. Недружественность (430-р) и перечень 2560-р категорию по ст.12 не меняют, но повышают риск запрета. Приказ РКН № 253 с 30.10.2026 сокращает перечень до 88 государств, исключена Украина.

265-ФЗ от 26.07.2026 и новый перечень стран

В силе с 26.07.2026: членство в Конвенции 108 само по себе адекватности не дает

Privacy Advocates

До 26.07.2026

- адекватны стороны Конвенции 108 и страны из перечня РКН
- для сторон Конвенции действовала отдельная оговорка в п.2 ч.5 ст.12
- перечень - приказ РКН № 128: 89 государств, 55 сторон Конвенции и 34 вне ее

С 26.07.2026

- ориентир один - перечень РКН, упоминания Конвенции исключены из чч.5, 10, 11 ст.12
- критерий включения: соответствие регулирования и применяемых мер положениям Конвенции
- запрет или ограничение по чч.7, 8, 12 ст.12 возможны по любой стране, как и раньше (РКН 14.08.2026)
- до 30.10.2026 действует приказ № 128, затем приказ № 253, и стороны Конвенции адекватны лишь как включенные в перечень

ПЕРЕЧЕНЬ СТРАН СЕЙЧАС

89 государств в приказе РКН № 128, действует до 30.10.2026, США и ОАЭ не входят

88 государств в приказе РКН № 253 от 16.09.2026, исключена Украина

253 приказ опубликован 19.10.2026, вступает в силу 30.10.2026, приказ № 128 утрачивает силу

Что сделать: инвентаризировать маршруты, которые опирались на членство страны в Конвенции, с 30.10.2026 проверять страну по приказу № 253, а для передач в Украину применять порядок для государств вне перечня и оценить судьбу поданных уведомлений.

Порядок ТПД с 01.03.2023

Категория страны определяет состав сведений и момент старта

Privacy Advocates

Намерение осуществлять ТПД

Страна в перечне РКН

Сведения от получателя

- наименование и контакты
- подтверждение конфиденциальности
- меры безопасности
- условия прекращения обработки

Уведомление РКН по ч.4 ст.12

старт сразу после уведомления

Страна вне перечня

Сведения от получателя

- наименование и контакты
- подтверждение конфиденциальности
- меры безопасности
- условия прекращения обработки
- **правовое регулирование ПД в стране**

Уведомление РКН по ч.4 ст.12

старт только после 10 рабочих дней

Случаи по ПП-2526

16 случаев: уведомление не подается вовсе

4 случая: спорт, культура и наука, платежи, связь - уведомление без права запрета

РКН вправе запретить и по своей инициативе (ч.8), и по представлению ведомств (ч.12, ПП-6)

РКН рассматривает 10 рабочих дней, +15 при запросе оценки (п.13 ПП-24)

Запрет или ограничение: прекратить и обеспечить уничтожение

Решения нет: передача начинается или продолжается

Подробная схема на Яндекс Диске

ТПД: порядок с 01.03.2023 и новеллы 2026 года

Оценка получателя, уведомление и 10 рабочих дней ожидания

Privacy Advocates

1. Основание	2. Оценка получателя	3. Уведомление РКН	4. 10 рабочих дней	5. Старт
ч.1 ст.6. Форма на Портале знает 7 оснований, иные на бумаге. Трудовой договор не основание	меры защиты и условия прекращения, для стран вне перечня обзор права, акт оценки	отдельно от уведомления по ст.22: цели, категории, страны, дата оценки	рассмотрение, запрос сведений о получателе: ответ за 10 дней, продление 5	страны из перечня - сразу после уведомления, иные - после срока без запрета

Запрет или ограничение

- возможны по любой стране, включая страны из перечня (РКН, 14.08.2026)
- основания решения регулятора - закрытый перечень ПП-24, межведомственные представления - ПП-6
- ПП-2526: в 16 случаях уведомление не подается, еще в 4 - без права запрета
- при запрете оператор обязан обеспечить уничтожение у получателя: это закрывает только договорная оговорка

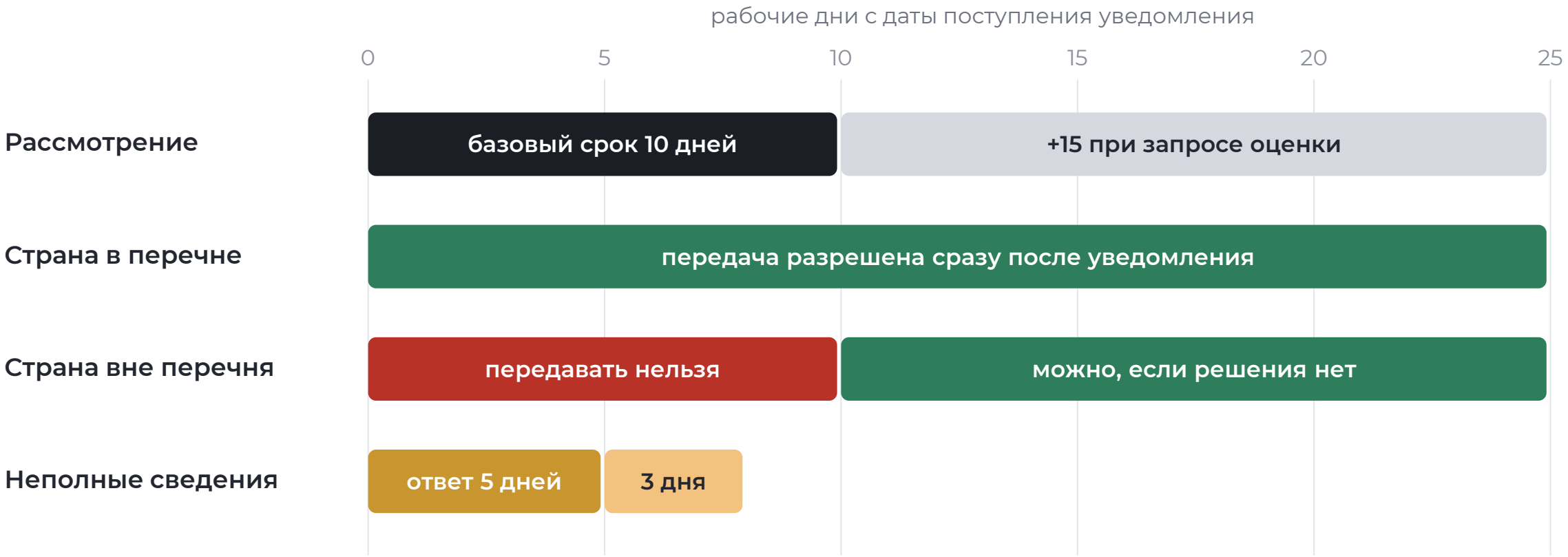
265-ФЗ от 26.07.2026

- в перечень включают по соответствию права и мер Конвенции № 108, само участие в ней больше не основание
- перечень меняется приказом без участия оператора: категорию страны отслеживают самостоятельно
- отдельного состава за неуведомление о ТПД нет: вменяют ч.1 ст.13.11, встречается и ч.10, главный риск - запрет и предписание

Сроки рассмотрения уведомления

Когда можно начинать передачу

Privacy Advocates



Неполные сведения: рассмотрение приостанавливается, ответ оператора 5 рабочих дней, возобновление не позднее 3 рабочих дней

Решение приходит письмом
с основаниями и рекомендациями, нет ответа - нет решения

5 рабочих дней
на представление ведомства по ПП-6

Повторная подача
после устранения причин, не ранее 10 рабочих дней после решения

Что получить от зарубежного получателя

Сведения по ч.5 ст.12 собираются до подачи уведомления

Privacy Advocates

Всем получателям

- полное наименование и контактные данные
- подтверждение конфиденциальности ПД
- меры по обеспечению безопасности обработки
- описание условий прекращения обработки

Плюс для стран вне перечня

Правовое регулирование ПД в стране получателя

- законодательство о ПД
- контроль и надзор за обработкой и защитой
- ответственность за нарушения
- участие в международных договорах о ПД
- иные вопросы по ожиданиям РКН

УСЛОВИЯ ПРЕКРАЩЕНИЯ ОБРАБОТКИ, КОТОРЫЕ СТОИТ ЗАФИКСИРОВАТЬ

достижение целей и сроков хранения | **незаконность или избыточность ПД** | **отзыв согласия или требование субъекта** | **запрос уполномоченного лица** | **иные условия по договору**

Оценка - компетенция оператора (РКН 06.12.2022): дата оценки в уведомлении не может быть позже даты его подачи.

Меры безопасности у получателя

Объем зависит от того, обрабатывает ли получатель ПД по поручению

Privacy Advocates

ТПД БЕЗ ПОРУЧЕНИЯ

5 базовых мер

1. определение угроз безопасности ПД
2. правовые, организационные и технические меры
3. восстановление ПД после инцидентов
4. регулярный контроль эффективности мер
5. уничтожение ПД с подтверждением

ТПД С ПОРУЧЕНИЕМ: 23 МЕРЫ ПО СТ.18.1 И 19 152-ФЗ

6 **Организация**
DPO, политика, локальные акты, процедуры по нарушениям, внутренний контроль, оценка вреда

8 **Защита в информационных системах**
угрозы, меры и СЗИ, оценка эффективности, правила доступа, журналы, контроль, ответственный

6 **Носители, помещения, люди**
места хранения и учет носителей, раздельные базы, режим помещений, перечень допущенных, обучение

3 **Инциденты и уничтожение**
реагирование на атаки, восстановление, уничтожение с подтверждением

Способы получения сведений

От открытых источников к экспертизе: чем глубже, тем надежнее оценка

Privacy Advocates

Политики получателя

общедоступные тексты о ПД и ИБ со снимком и датой

Договоры

проекты и заключенные договоры об обработке или передаче

Запрос документации

документы о защите ПД, для стран вне перечня - о праве страны

Интервью или анкета

форму запроса оператор выбирает сам (РКН 15.05.2024)

Правовая экспертиза

анализ права страны вне перечня, своими силами или внешний

глубина и надежность оценки

Фиксируйте процесс и результат: отказ или молчание получателя тоже результат оценки.

Переложите работу на получателя: договор обязывает готовить сведения и сообщать об их изменениях.

Риски ТПД и управление ими

Запрет, ограничение и задержка старта идентифицируются до уведомления

Privacy Advocates

Запрет

п.23 ПП-24

- получатель не защищает ПД или не определил условия уничтожения
- получатель - запрещенная судом РФ организация
- получатель - нежелательная в РФ НПО
- ТПД несовместима с целями сбора
- ТПД не предусмотрена ч.1 ст.6

Ограничение

п.26 ПП-24

- содержание и объем ПД не соответствуют цели
- категории субъектов не соответствуют цели

Задержка старта

практика

- нет уведомления об обработке по ст.22
- страна вне перечня РКН
- биометрия, спецкатегории, обезличенные ПД, ПД детей
- основания нет в электронной форме - подача на бумаге
- цель ТПД отличается от цели сбора



Первым шагом проверяются ранее принятые решения о запрете или ограничении ТПД (чч.8, 12 ст.12, ПП-6).

Если РКН запретил или ограничил ТПД

Последствия решения и способы защиты оператора

Privacy Advocates

Решение РКН: письмо с основаниями

Запрет
заявленная передача невозможна в полном объеме

Ограничение
передача в скорректированных целях, субъектах и составе ПД

Обеспечить уничтожение переданных ПД получателем (ч.14 ст.12): рычаг только договорный, порядок и подтверждение уничтожения закладываются заранее.

СПОСОБЫ ЗАЩИТЫ

Обжалование
в суд или вышестоящему должностному лицу, жалоба в течение месяца

Повторное уведомление
после устранения причин, не ранее 10 рабочих дней после решения

Решение по представлению
по ПП-6 - обращение о снятии в ведомство, внесшее представление

Генетические данные: отдельный порядок с 01.09.2026

ПП РФ от 15.06.2026 № 750 во исполнение ст.13.1, 13.2 86-ФЗ

Privacy Advocates

Данные популяционных генетических и иммунологических исследований иностранным лицам, их филиалам и представителям не передаются, в том числе внутри РФ, кроме исключительных случаев по решению комиссии.

1 Свободный

медпомощь конкретному пациенту, препараты и БМКП для пациента при медицинской лицензии, международное сотрудничество

без согласования

2 Уведомительный

популяционные исследования с публикацией сводных показателей

уведомить комиссию не позднее чем за 20 рабочих дней

3 Разрешительный

прочие случаи

решение комиссии за 15 рабочих дней, возможно продление

Комиссия при Правительстве
возглавляет вице-премьер по здравоохранению, работу обеспечивает ФМБА, плата не взимается

Отказ по закрытому перечню
неполнота сведений, риски для прав граждан, риски биобезопасности

Параллельно ст.12 152-ФЗ
через комиссию данные передаются в обезличенной форме

РАЗДЕЛ 20. ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПД

20.3

Уведомление о намерении

Содержание, цель, ошибки и сопровождение

- содержание и цель ТПД
- типичные ошибки и изменения
- договор и реестр потоков

Содержание уведомления о намерении

Восемь сведений по ч.4 ст.12 152-ФЗ, отдельная форма нормативно не утверждена

Privacy Advocates

Уведомление о намерении осуществлять ТПД

1. **Наименование и адрес оператора**
2. **Дата и номер уведомления об обработке ПД**
3. **ФИО и контакты ответственного (DPO)**
4. **Правовое основание и цель ТПД**
5. **Категории и перечень передаваемых ПД**
6. **Категории субъектов ПД**
7. **Перечень иностранных государств**
8. **Дата оценки допустимости ТПД**

ОСНОВАНИЯ В ЭЛЕКТРОННОЙ ФОРМЕ

- согласие субъекта
- международный договор или закон
- правосудие и исполнительное производство
- исполнение акта органа власти
- договор с субъектом
- журналистика и СМИ
- статистика и исследования

Законного интереса в форме нет: такое основание заявляется на бумаге, что сдвигает старт.

Дата оценки не может быть позже даты подачи уведомления, а уведомление не заменяет правовое основание.

Как сформулировать цель ТПД

Цель описывает причину передачи, а не норму и не основание

Privacy Advocates

Так нельзя

Соблюдение законодательства РФ	расплывчато
Трудовой кодекс РФ	НПА без нормы
Согласие субъекта ПД	основание вместо цели
Обработка ПД работников и клиентов	смешаны субъекты

Так можно

Бронирование билетов и гостиниц для командировок работников	работники
Подготовка отчетности о составе органов управления для материнской компании	члены органов
Анализ посещаемости сайта с помощью сервиса веб-аналитики	посетители сайта
Техническая поддержка ERP иностранным подрядчиком	пользователи ERP

Одна цель - одна категория субъектов
работники отдельно от клиентов

Макроцель раскрывается микроцелями
по процессам и получателям

Работники: основание спорно
РКН 2024 - согласие по ст.88 ТК, 2025-2026 - для командировок можно без согласия

Типичные ошибки в уведомлениях о ТПД

Семь ошибок по данным РКН и девять ошибок из практики

Privacy Advocates

РОСКОМНАДЗОР

7 типичных ошибок

1. избыточные передаваемые ПД
2. ПД не соответствуют цели
3. дата оценки получателя позже даты подачи уведомления
4. неполный перечень сведений по ч.4 ст.12
5. цель сформулирована расплывчато
6. целью указаны НПА без привязки к норме
7. целью указано правовое основание

t.me/rkn_tg/724

Инвентаризация

- выявлены не все случаи ТПД, страна серверов получателя не учтена
- не учтены планы изменения ТПД
- не различены ТПД с поручением и без него, в страны перечня и вне его

Оценка получателя

- избыточный запрос сведений или анкета как единственный способ
- оценка допустимости ТПД приравнена к оценке одного получателя
- процесс и результаты оценки не задокументированы

Документы

- в договоре нет условий о ТПД и уничтожении ПД при запрете
- нет актуального уведомления по ч.1 ст.22
- основание ТПД не соотнесено с целью и категорией субъектов

Направление уведомления

Электронная форма на портале ПД или бумага, одно уведомление на направление деятельности

Privacy Advocates

1 Портал ПД	2 Заполнение	3 Подписание	4 Ожидание
pd.rkn.gov.ru, раздел трансграничной передачи	по образцу РКН, поля ч.4 ст.12	ЭП или распечатка с отправкой по почте	решение приходит письмом, нет письма - нет решения

Одно уведомление на направление
совокупность цели, стран, категорий и объема ПД, а не каждый факт или контрагент (РКН 06.12.2022)

Реестр операторов не условие
уведомление о ТПД подается и без уведомления об обработке, но его отсутствие - самостоятельное нарушение

Синхронизация трех документов
уведомление о ТПД, уведомление об обработке и политика: цели, ПД, субъекты и факт передачи совпадают

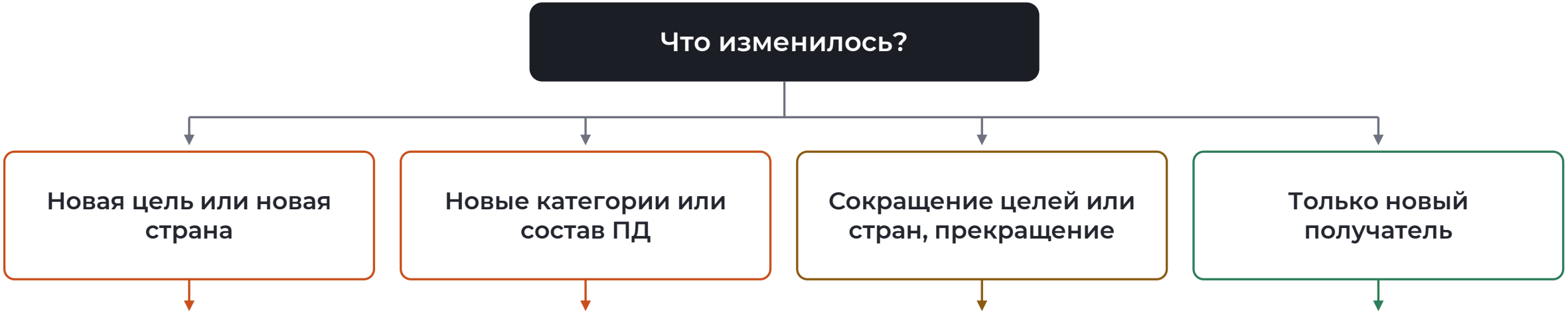
Уведомление не основание
правомерность передачи держится на основании из ч.1 ст.6, уведомление его не заменяет

Форма: pd.rkn.gov.ru/cross-border-transmission/form2 **Образец:** pd.rkn.gov.ru/docs/primer_zapolnenija_uvedomlenija_TPdn.pdf

Как уведомить об изменениях ТПД

Процедуры изменения нет ни в 152-ФЗ, ни на портале ПД

Privacy Advocates



Совет: закладывайте в уведомление обозримые планы, а решение о подаче или неподаче нового уведомления фиксируйте в реестре трансграничных потоков.

Роскомнадзор о новом порядке ТПД

Ответы РКН на вебинаре 15.05.2024 и уточнения 14.08.2026

Privacy Advocates

? Какую страну указывать?

В 2024 году - страну регистрации получателя. С 14.08.2026 учитываются и страна регистрации, и страна серверов.

? Когда подавать новое уведомление?

При новой цели, стране или категориях ПД, а при сокращении целей или стран - тоже целиком.

? Как запрашивать сведения?

Форму запроса выбирает оператор: письмо, анкета, интервью или документы получателя.

? Зарубежный филиал российского юрлица?

В 2024 году РКН считал передачу ему ТПД, в 2022, 2023 и 2025 годах высказывался иначе.

? Сменился только получатель?

Нового уведомления не нужно, но сведения по ч.5 ст.12 у нового получателя запрашиваются заново.

? Можно ли запретить ТПД в адекватную страну?

Да, запрет и ограничение по чч.7, 8, 12 ст.12 от категории страны не зависят (14.08.2026).

Переподавать ли уведомления под новый перечень стран?

Решение принимается по каждому направлению и документируется

Privacy Advocates

За переподачу

- закрывает спор о судьбе уведомления при смене категории страны ✓
- актуализирует цели, состав ПД и страны, включая страну серверов получателя ✓
- синхронизирует уведомление с обновленной оценкой получателя ✓



Против

- ✗ закон не требует нового уведомления, если цели, страны и состав ПД прежние
- ✗ до 30.10.2026 действует приказ № 128, мотивы исключения Украины не опубликованы
- ✗ по стране вне перечня новые передачи стартуют только после срока рассмотрения

Смена перечня не запрещает передачу

Для страны, исключенной из перечня, меняются момент старта новых передач (после 10 рабочих дней рассмотрения) и состав сведений о получателе: добавляется правовое регулирование ПД в стране.

Сопутствующая ТПД: уведомлять ли о переписке?

Контакты работников неизбежно уходят за рубеж при оценке получателя

Privacy Advocates

Вопрос оператора

Деловая переписка с иностранным получателем ради сбора сведений о его мерах защиты передает за рубеж контакты работников оператора.

Нужно ли отдельное уведомление или такая передача носит сопутствующий характер?

Позиция автора: сопутствующую ТПД ради исполнения ст.12 можно не выделять, но регуляторы строже.

ПОЗИЦИИ РЕГУЛЯТОРОВ

07.04.2023 Минцифры, П25-7258-ОГ — ТПД

контакты работника в переписке на иностранный почтовый сервер - ТПД

01.03.2023 РКН, устно — частично

только номера телефонов - не ТПД, адреса электронной почты - ТПД

01.06.2023 РКН, 08-46101 — ТПД

контакты в деловой переписке с иностранным лицом - ТПД с уведомлением

2026 Управление РКН по СКФО — не ТПД

минимальные служебные данные без возможности идентификации - не ТПД

Безопасный вариант: включить деловую переписку с зарубежными контрагентами в уведомление отдельной целью.

Формализуем условия ТПД в договоре

Договор - единственный рычаг оператора на зарубежного получателя

Privacy Advocates

Соглашение о трансграничной передаче ПД

1. **Предмет.** цели ТПД, состав ПД и категории субъектов
2. **Сведения по ч.5 ст.12.** обязанность предоставить их и сообщать об изменениях
3. **Меры защиты.** конфиденциальность и меры безопасности
4. **Инциденты.** немедленное сообщение оператору, у него 24 и 72 часа
5. **Запрет РКН.** прекращение передачи и уничтожение ПД по ч.14 ст.12
6. **Уничтожение.** сроки, порядок и подтверждение уничтожения
7. **Дальнейшая передача.** только с согласия оператора
8. **Поручение.** условия ч.3 ст.6, если получатель - обработчик

DTA

Получатель - самостоятельный оператор: сам определяет цели и средства обработки и сам отвечает перед субъектом.

DPA

Получатель действует по поручению: иностранный обработчик отвечает перед субъектом солидарно с оператором (ч.6 ст.6).

Без договора уничтожение ПД при запрете РКН обеспечить нечем: порядок и подтверждение закладываются заранее.

Реестр трансграничных потоков

Внутренний документ, который связывает ст.12 с доказательствами соблюдения

Privacy Advocates

Передача					Оценка	Уведомление	Контроль
Поток	**Страна и категория**	**Получатель**	**Цель**	**ПД и субъекты**	**Оценка**	**Уведомление**	**Пересмотр**
Веб-аналитика	США, вне перечня	Google LLC	анализ посещаемости сайта	идентификаторы, cookie, посетители	политика, DPA	решения нет, старт через 10 дней	ежегодно
Отчетность группе	Германия, в перечне	материнская компания	отчетность о составе органов	ФИО, должность, члены органов	запрос документов	старт сразу	при смене состава
Техподдержка ERP	Индия, в перечне	подрядчик	поддержка ERP	ФИО, логин, пользователи	анкета, договор	старт сразу	при смене подрядчика

пример заполнения

СИНХРОНИЗАЦИЯ ТРЕХ ДОКУМЕНТОВ

Уведомление о ТПД — **Уведомление об обработке** — **Политика на сайте**

Цели, ПД, субъекты и факт передачи совпадают во всех трех документах.

Отдельный реестр не обязателен: достаточно добавить поля ТПД в реестр процессов обработки.

20.4

Практика и ответственность

Статистика РКН, санкции и судебные акты

- статистика рассмотрения уведомлений
- административный и уголовный риск
- дела 2024-2026

Ответственность за нарушения порядка ТПД

Отдельного состава за неуведомление о ТПД нет, квалификация разнится

Privacy Advocates



Предписание РКН о приостановке или запрете ТПД (п.4 ч.3 ст.23 152-ФЗ) плюс репутационный вред.

Риск квалификации: одно неуведомление прокуроры и суды оценивают по ч.1, ч.10 или ч.8 ст.13.11 и по ст.19.7.

Практика 2024-2026

Прокуроры, суды и Конституционный суд о нарушениях порядка ТПД

Privacy Advocates

18.06.2024 — **Мировой судья, уч. № 351, Москва**

прокурор: ТПД данных работников, претензии к согласию, ч.2 ст.13.11

штраф 100 тыс. ₽

08.09.2025 — **АС Республики Башкортостан, А07-27941/2025**

прокурор: зарубежные поездки детей без уведомления о ТПД, ч.10 ст.13.11

предупреждение

2026 — **Мировой судья, уч. № 113 Абинского района**

иностранная платформа на сайте администрации, вменена ч.8 ст.13.11

100 тыс. ₽ ДЛ

09.06.2026 — **АС г. Москвы, А40-325054/2025, Taobao**

локализация по ч.8 ст.13.11, ст.12 в мотивировке, апелляция 29.09.2026

штраф 1 млн ₽

30.06.2026 — **КС РФ, № 2027-О, дело А40-238444/2024**

перенос данных заказчика на зарубежные серверы провайдером - злоупотребление правом

жалоба не принята

Уголовный риск: ст.272.1 УК

Незаконные использование и передача компьютерной информации с ПД, с 11.12.2024

Privacy Advocates

СОСТАВ

ч.1 использование, передача, сбор и хранение компьютерной информации с ПД, полученной незаконно

ч.4 те же деяния, сопряженные с ТПД или трансграничным перемещением носителей, - квалифицирующий признак

прим. 2 перемещение носителей - ввоз и вывоз машиночитаемого носителя с ПД, независимо от передачи иностранцу

ГРАНИЦА С АДМИНИСТРАТИВНОЙ ОТВЕТСТВЕННОСТЬЮ

КоАП

нарушен порядок обработки законно полученных ПД: нет уведомления, основания, оценки

УК

информация получена незаконно, а ТПД или вывоз носителя усиливают ответственность

Что сделать

- подтверждать законность источника ПД, особенно купленных и полученных от партнеров
- вести учет носителей с ПД и шифровать ноутбуки для поездок
- не использовать для ТПД выгрузки, происхождение которых не подтверждено

Дорожная карта ТПД

Шесть шагов, которые повторяются при каждом изменении потоков

Privacy Advocates



Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
LOK-025	[2026] Штраф 100 тыс. ₽ на должностное лицо	19 Локализация

20.5

Практикум

Восемь ситуаций и дорожная карта

- Практикум: квалифицируйте ситуации
- Практикум: ответы

Практикум: квалифицируйте ситуации

Есть ли ТПД, нужно ли уведомление и нет ли нарушения локализации?

Privacy Advocates

1. Интернет-магазин использует Google Analytics
2. Аудитор материнской компании из Германии получает удаленный доступ к HR-системе в РФ
3. Работник - гражданин РФ в командировке в Казахстане открывает CRM в РФ
4. Отдел продаж ведет Google-таблицу с клиентами, выгруженными из CRM в РФ
5. Компания публикует новости с ФИО сотрудников в своем Telegram-канале
6. Головному офису в США отправлен пакет корпоративных документов с ПД директоров
7. Клиника передает генетические данные пациента в зарубежную лабораторию для подбора лечения
8. Передача филиалу российской компании в Армении, не являющемуся юрлицом по местному праву

Практикум: ответы

Квалификация и опора по каждой ситуации

Privacy Advocates

1	ТПД	ТПД с уведомлением, а если ПД попадают в сервис раньше, чем в БД в РФ, еще и нарушение локализации	РКН 04.08.2025 № 08-373883, 22.01.2026
2	ТПД	ТПД, Германия в перечне: передача возможна сразу после направления уведомления	п.11 ст.3, чч.3, 10 ст.12
3	не ТПД	не ТПД: получатель не иностранное лицо	п.11 ст.3
4	локализация	не ТПД по позиции РКН, но нарушение ч.5 ст.18	РКН 01.11.2025, 12.01.2026
5	не ТПД	не ТПД: распространение неопределенному кругу, но нужно согласие на распространение	пп.5, 11 ст.3, ст.10.1 152-ФЗ
6	ТПД	ТПД, США вне перечня: передача только после 10 рабочих дней рассмотрения	ч.11 ст.12, приказ РКН № 253
7	ПП-750	ПП-750: свободный маршрут при медицинской лицензии плюс ст.12 в части ПД	ПП-750, ст.12 152-ФЗ
8	спорно	спорно: РКН 01.03.2023 и 27.08.2025 - не ТПД, 15.05.2024 - ТПД	устные позиции РКН

КЛЮЧЕВЫЕ ВЫВОДЫ

- ТПД - передача из РФ иностранному лицу на территорию иностранного государства, пересечение границы признаком не является, спорные зоны решаются в пользу строгой позиции.
- До передачи: основание из ч.1 ст.6, сведения от получателя по ч.5 ст.12 и уведомление, для стран вне перечня - выдержка 10 рабочих дней.
- 265-ФЗ оставил один ориентир - перечень РКН, а запрет или ограничение возможны по любой стране.
- Реестр потоков, договор с получателем и синхронизация документов превращают разовое уведомление в устойчивое соответствие.

21

Поручение и передача третьим лицам

Поручение, передача, DTA, проверка контрагента и группа компаний

21.1 Поручение или передача

21.2 Условия поручения и контроль обработчика

21.3 Передача оператору и DTA

21.4 Проверка контрагента

21.5 Группа компаний

Раздел на сайте
privacy-advocates.ru/pd/por

21.1

Поручение или передача

- Роль получателя задает цель, а не название договора
- Поручение возникает там, где у подрядчика есть доступ

Роль получателя задает цель, а не название договора

Пять шагов выбора документа под передачу и три исхода квалификации получателя

Privacy Advocates

1 **Основание передачи**

у передающей стороны по ч.1 ст.6: согласие, договор с субъектом, закон

2 **Возникает ли роль**

ответ органу и собственная услуга субъекту поручения не образуют

3 **Критерий цели**

нет своей цели - обработчик, своя цель и отношения с субъектом - оператор

4 **Поток за потоком**

одно лицо бывает обработчиком и оператором по разным потокам

5 **Документ**

поручение, соглашение о передаче или письменный вывод

ИСХОД	ПРИЗНАК	ТИПИЧНЫЕ ПРИМЕРЫ	ДОКУМЕНТ
обработчик	нет собственной цели, обслуживающая функция	бухгалтерия и расчет зарплаты, колл-центр, хостинг и техподдержка, рассылки, пропускной режим	поручение по ч.3 ст.6
оператор	своя цель и прямые отношения с субъектом	банк зарплатного проекта, ДМС, медосмотры, корпоративное такси, кадровое агентство (РКН, 19.08.2025)	DTA и основание передачи
без новой роли	собственная обязанность каждого по закону	ответ на запрос органа (п.2 ч.1 ст.6), клиринг и центральный контрагент (Банк России, 27.08.2024)	вывод в реестре обработки

Важно: отдельного режима обработчика в России нет: он тоже оператор (п.7 ПП-1046) и получает лишь три послабления - согласие не собирает, перед субъектом за него отвечает оператор, сам он отвечает перед оператором

Поручение возникает там, где у подрядчика есть доступ

Облако, хостинг, обслуживание и посредники: граница поручения и расхождение с Роскомнадзором

Privacy Advocates

Четыре признака обработчика | цель в отношении содержания | осведомленность о ПД | доступ к содержанию | самостоятельные действия с данными

КОНТРАГЕНТ	ЭКСПЕРТНЫЙ ПОДХОД	РЕГУЛЯТОР И СУДЫ
SaaS: CRM, кадровый ЭДО, аналитика, модели ИИ	обработчик	поручение
IaaS и выделенный сервер без доступа к данным	посредник	поручение и без доступа: Управление Роскомнадзора по Курской области, 18.06.2026
Хостинг и техподдержка сайта	обработчик	поручение, предписание устояло в первой инстанции (А49-14214/2022)
Обслуживание ПО при парольном разграничении	не обработчик	доступ не доказан, предписание недействительно (А16-1293/2011, апелляция 15.05.2012)
Архив с описью, поиском и сканированием	обработчик	доступ выведен из прайс-листа, предписание законно (А40-32030/2016, апелляция 02.08.2016)

Довод: презумпцию доступа опровергает архитектура, например ключ шифрования только у клиента, а не договорный запрет. Уклониться от поручения ради меньшей ответственности нельзя

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
BAZ-012	Взаимодействие между основными лицами	03 Обзор комплаенса
BAZ-013	Поручение или передача: что фиксирует соглашение	03 Обзор комплаенса
SAJ-009	Поручение нужно инфраструктуре сайта, а не каждому виджету	22 Сайт
AIG-011	Поставщик ИИ: обработчик или оператор	24 ИИ и ПД
LOK-028	Кому передавать: оператору, а не обработчику	19 Локализация

21.2

Условия поручения и контроль обработчика

- Условия поручения пишут предметно, а не отсылкой к статьям
- Согласие на поручение называет обработчика поименно
- Обработчика контролируют на всех этапах, а отвечает оператор
- Шесть спорных вопросов поручения без устойчивого ответа

Условия поручения пишут предметно, а не отсылкой к статьям

Минимум ч.3 ст.6 152-ФЗ и формулировки, которые делают поручение инструментом контроля

Шаблон DPA
скачать

Privacy Advocates

УСЛОВИЕ	НОРМА	КАК СФОРМУЛИРОВАТЬ
Цель и перечень ПД	ч.3 ст.6	дословно по согласию субъекта или уже: выйти за рамки согласия нельзя
Перечень действий	ч.3 ст.6	без него поручение нарушает закон, такой пункт предписания устоял в кассации (А40-81171/2017)
Конфиденциальность и меры	ст.7, 18.1, 19	уровень защищенности по ПП-1119, а для бумаги правила ПП-687 вместо требований к ИСПД
Документы по запросу	ч.3 ст.6	право на аудит: сроки ответа, выезд, сторонний аудитор, расходы при нарушениях
Инциденты	ч.3.1 ст.21	обработчик сообщает за 12 и 48 часов при 24 и 72 у оператора и без решения оператора молчит вовне
Локализация	ч.5 ст.18	по редакции с 01.07.2025, поручения, заключенные раньше, обновляют
Прекращение	ст.21, приказ № 179	уничтожение за 5 рабочих дней с подтверждением, срок не привязан к сроку услуг

Риск: Роскомнадзор 07.08.2025 назвал отсылочное поручение недостаточным. Дефект обычно наказывают предписанием, а затем ст.19.5 КоАП, и зарубежный шаблон без российского минимума этот риск не снимает

Согласие на поручение называет обработчика поименно

Когда согласие нужно, как оформить его с 01.09.2025 и чем покрыть субобработку

Privacy Advocates

Письменная форма

Работники, спецкатегории, биометрия

- одна цель и одно лицо по поручению с наименованием и адресом (п.6 ч.4 ст.9)
- перечень возможных обработчиков наименования не заменяет (А40-32030/2016)
- при замене подрядчика согласие переоформляют, а не дополняют
- Роскомнадзор ждет подписи по каждому обработчику или категории получателей

vs

Обычная форма

Иные случаи согласия

- обработчика можно раскрыть отсылкой к списку на сайте (позиции 27.07.2023, 22.10.2025, 14.08.2026)
- с 01.09.2025 согласие оформляют отдельным документом, а не строкой договора
- договор с субъектом сам бывает основанием, но Роскомнадзор 07.08.2025 называл согласие
- субобработчик допустим, только если право предусмотрено поручением и охвачено согласием

Подход PA: в согласии работника цели объединяют в блоки, третьих лиц - в категории с обработчиками поименно и получателями без имен, а подпись или отметку ставят по каждой категории. Поручение без согласия ведет к предписанию об уничтожении (А56-82428/2022, апелляция 20.03.2023)

Обработчика контролируют на всех этапах, а отвечает оператор

До доступа, во время обработки, при инциденте и после поручения: что заложить в договор

Privacy Advocates

до

ДОСТУП

Проверка и минимизация

чек-лист по типу передачи, лишние поля не передают, передачу отражают в реестре и политике

во время

КОНТРОЛЬ

Аудит и карта цепочки

аудит раз в 1-3 года, перечень субобработчиков, сверка договора с фактическим потоком

инцидент

СРОКИ

Сообщить раньше закона

отсчет 24 и 72 часов может запустить сам обработчик, совместного уведомления нет

после

ВЫХОД

Уничтожить и подтвердить

уничтожение по любому основанию прекращения, блокирование до 6 месяцев, возврат носителей

ЧЧ.5, 6 СТ.6

Перед субъектом отвечает оператор

- утечка у подрядчика - ответственность оператора перед субъектом и Роскомнадзором
- к подрядчику после возмещения остается регресс
- иностранный обработчик отвечает перед субъектом вместе с оператором

ДОГОВОР

Распределить последствия заранее

- предел ответственности подрядчика - не ниже первого вероятного штрафа оператора
- обработчику штраф может прийти самостоятельно, хотя Роскомнадзор относит его на оператора
- аффилированность в группе ни одной обязанности не снимает

Шесть спорных вопросов поручения без устойчивого ответа

Где позиции Роскомнадзора, судов и экспертов расходятся и какой вариант осторожнее

Privacy Advocates

? Одно поручение нескольким обработчикам?

Роскомнадзор 01.03.2023 требовал отдельное поручение на каждого, а устно 14.08.2026 допустил нескольких при общей цели в договоре. Осторожно - отдельный документ

? Нужно ли называть субобработчика?

закон молчит, а Роскомнадзор требует предусмотреть право привлечения в поручении и согласии. Осторожно - раскрывать цепочку перечнем

? Можно ли поручить без согласия, на законном интересе?

единичные дела допускали пп.5 и 7 ч.1 ст.6, но ч.3 ст.6 требует согласия, если закон не говорит иное. Устойчивой практики нет

? Возникает ли поручение без подписанного договора?

письменная форма соблюдается и набором документов, например офертой и перепиской. Отсутствие единого текста поручения не отменяет

? Отвечает ли оператор за невиновную утечку у подрядчика?

судья ВС 21.01.2026 оставил штраф Минтруда: доказательств внутреннего контроля и защиты в деле не было. Вину оценивают через собственные меры

? Поручение или передача по данным работников?

ст.88 ТК требует от получателя подтверждения целей, что неисполнимо для банка или страховщика. Практика норму фактически не применяет

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OTV-026	Минтруд: ошибка подрядчика не спасает оператора от штрафа	30 Ответственность

21.3

Передача оператору и DTA

- Передачу самостоятельному оператору оформляют DTA, а не NDA
- Зарплатный банк выбирает работник, а не работодатель
- База ПД не товар: любая ее передача требует своего основания
- Передача состоялась, когда у получателя появился доступ

Передачу самостоятельному оператору оформляют DTA, а не NDA

Рамочное межоператорское соглашение: опоры в законе, основание передачи и одиннадцать блоков

Privacy Advocates

DATA TRANSFER AGREEMENT

Соглашение о передаче без поручения

двустороннее, взаимное, бессрочное, подписывается однократно. Прямой нормы нет, но передачу вне поручения подпирают ст.7, п.1 ч.4 ст.18, ч.3 ст.20 и п.11 ст.3

- NDA защищает коммерческую тайну и правомерность передачи ПД не покрывает
- основание остается у передающей стороны: договорное - только если субъект сторона или выгодоприобретатель (п.5 ч.1 ст.6)

СОСТАВ СОГЛАШЕНИЯ

1. стороны как самостоятельные операторы
2. предмет и состав передаваемых ПД
3. заверения об основаниях и уведомлении субъектов
4. прекращение при утрате оснований
5. конфиденциальность и меры безопасности
6. инциденты: взаимно 12 и 48 часов, вовне после консультаций
7. содействие при обращениях и проверках
8. право получателя обрабатывать самостоятельно и поручать
9. приложение о ТПД по условию
10. заверения, ответственность, право
11. бессрочность и действие на прошлые отношения

Data Transfer Addendum
скачать

Шаблон DTA
скачать

Срок: разумный срок взаимодействия привязывают к законным срокам зависящей стороны, иначе обязательство без срока исполняется за 7 дней по ст.314 ГК. Опосредованную передачу через третье лицо соглашением тоже охватывают

Зарплатный банк выбирает работник, а не работодатель

Ответы Роструда 15.09.2026 и 07.10.2026: передача данных в банк и выпуск карты без заявления незаконны

Privacy Advocates

Так можно

- зарплата идет в банк из письменного заявления работника (ч.3 ст.136 ТК)
- работник меняет банк, сообщив реквизиты не позднее чем за 15 календарных дней до выплаты
- данные для выпуска карты передают в банк только после заявления работника

vs

Так нельзя

- перечислять зарплату в выбранный работодателем банк без волеизъявления
- выпускать карту и передавать данные в банк до заявления и согласия
- ежемесячно самому выбирать банк-получатель

Оговорка: Роструд оценивал по трудовому законодательству и оценку по 152-ФЗ оставил Роскомнадзору. Нужна ли отдельная письменная форма согласия, спорно: Роструд в 2015 году требовал ее, Роскомнадзор устно считает достаточным заявление

База ПД не товар: любая ее передача требует своего основания

Сделки с базами, M&A и группа компаний: где передача требует собственного основания

Privacy Advocates

сделка с массивом

Не купля-продажа

- конструкции - услуга по обработке, доступ или лицензия на базу данных
- заверения об основаниях по категориям субъектов (ст.431.2 ГК)
- отозвавших согласие исключают на дату передачи, а не выгрузки
- покупка без проверки происхождения - риск ничтожности (п.2 ст.168 ГК), истцом выступит регулятор

M&A

Изъятия для сделки нет

- до перехода контроля покупателю дают обезличенные и агрегированные показатели
- юридическая проверка сделки аудит ПД не заменяет
- выявленное закрывают заверениями и возмещением потерь (ст.406.1 ГК)
- реорганизация повторного согласия не требует

группа компаний

Группа - не субъект права

- каждое юрлицо - оператор, внутригрупповые потоки инвентаризируют и оформляют
- передача иностранной материнской компании - ТПД
- справочник группы без согласия - только при общем функционале (позиция 22.08.2025)
- совместное предприятие оформляют как внешний контур

Передача состоялась, когда у получателя появился доступ

Операционная модель управления передачами, учет раскрытий и запись получателей в политике

Privacy Advocates

1. **Процесс и основания**
   передача есть в реестре обработки, совместима с целью сбора, субъект о ней знает
2. **Договорная модель**
   роли сторон и базовые условия, если передача идет не в силу закона
3. **Учет передач**
   единое описание и перечень внешних интерфейсов: тип, направление, частота, объем
4. **Прозрачность**
   политика и реестр до начала передачи, контекстное уведомление в момент действия
5. **Риски и безопасность**
   оценка как операции повышенного риска, договорные меры реализованы технически

ПЕРЕДАЧА

- ✓ ключ к API, учетная запись подрядчика, VPN, общая папка или дашборд - с момента выдачи доступа
- ✓ учетная запись работника во внешней системе - передача ее оператору

НЕ ПЕРЕДАЧА

- ✗ доступ только на запись, например бот, регистрирующий обращения
- ✗ поступление данных от своего обработчика: их собрал сам оператор

Типовой пробел: в учет часто попадает только отправка файлов, а доступы бывших подрядчиков годами нигде не значатся. В политике получателей записывают функцией, органы - поименно

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OTV-032	Передача ПД работника бухгалтеру и арендодателю не требует согласия	30 Ответственность
TPD-032	Формализуем условия ТПД в договоре	20 ТПД

21.4

Проверка контрагента

- Контрагента проверяют до доступа и по типу передачи
- Проверка контрагента сама является обработкой ПД

Контрагента проверяют до доступа и по типу передачи

Чек-лист для третьих лиц: базовые критерии и требования при поручении и ТПД

Чек-лист третьих лиц
скачать

Privacy Advocates

ЖИРНЫМ - ОБЯЗАТЕЛЬНЫЕ КРИТЕРИИ: БЕЗ НИХ ОДОБРЕНИЯ НЕТ

любая передача

Базовые

- **реестр операторов или уведомление**
- **политика с целями и сроками**
- **нет санкций и предписаний за год**
- **назначен ответственный**
- **готов подписать DTA**
- нет утечек за 3 года
- сертификаты и аттестаты ИБ

поручение

Плюс для обработчика

- **готов подписать DPA с аудитом, субподрядом и инцидентами**
- **подтвердил уровень защищенности по ПП-1119**
- план реагирования на инциденты
- обучение персонала
- нет санкций за год
- страховка или гарантия

ТПД

Плюс для иностранного получателя

- **не запрещен и не нежелателен, нет запрета ТПД**
- **готов подписать приложение о ТПД со сведениями ч.5 ст.12 и уничтожением при запрете**
- сведения о мерах защиты, а для стран вне перечня и о правовом режиме, получают до уведомления о ТПД

Зачем: отметку "неприменимо" ставят с обоснованием, оценку пересматривают раз в 3 года. Задокументированная осмотрительность - довод о принятии всех мер (ч.2 ст.2.1 КоАП)

Проверка контрагента сама является обработкой ПД

Основание и объем по цели, представители по доверенности, сроки хранения и аутсорсинг проверки

Privacy Advocates

Основание

законный интерес (п.7 ч.1 ст.6), а идентификация по 115-ФЗ - в силу закона (п.2 ч.1 ст.6)

Объем по цели

для полномочий хватает данных руководителя и представителя, бенефициары - для аффилированности и противолегализационных проверок

Не собирать

копии паспортов работников контрагента вне 115-ФЗ и профили соцсетей как общедоступные

Представители

данные доверенности обрабатывают в силу представительства, согласие представителя не требуют

Сроки

данные несостоявшегося контрагента уничтожают, материалы проверки хранят на срок договора и давности

Справка из базы

основание поставщика комплаенс-сервиса к клиенту не переходит

КЕЙС PRIVACY ADVOCATES

Аутсорсинг проверки сервисной компании группы

- вынос преддоговорной проверки вовне - поручение с ответственностью оператора по ч.5 ст.6
- нужны согласия проверяемых лиц, с которыми отношений еще нет и которые вправе их отозвать
- на операторе остаются аудит исполнителя, сроки по инцидентам и уничтожение у него
- аффилированность компаний рисков не снимает
- выход - оставить проверку в периметре или строить исполнителя самостоятельным оператором

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
TPD-018	Что получить от зарубежного получателя	20 ТПД

21.5

Группа компаний

- Внутри группы каждый поток получает свой документ
- Право на документы общества зависит от статуса, а не от наличия ПД
- Из выдаваемого участнику документа ПД не вымарывают
- Данные связанных лиц собирают по норме, а не впрок

Внутри группы каждый поток получает свой документ

Позиции РКН по типовым потокам холдинга: учет, справочник, обучение, подразделения, доступ извне

Privacy Advocates

ПОТОК	КВАЛИФИКАЦИЯ	ЧТО ОФОРМИТЬ
Централизованный кадровый и бухгалтерский учет	делегирование полномочий оператора, то есть поручение (РКН устно, 28.01.2022 и 22.10.2025)	договор поручения и согласие работников на передачу
Филиал, представительство, иное обособленное подразделение	филиал оператором не является, иное подразделение РКН устно (22.08.2025) считает отдельным оператором, что спорно по п.2 ст.3	вести такие подразделения самостоятельными операторами
Общий справочник и мессенджер группы	без согласия при общем функционале или едином процессе (РКН устно, 22.08.2025)	письменная позиция строже: письмо РКН от 20.02.2025 № 08-72692 требует согласия по ст.8, опора на устную рискованна
Обучение работников франчайзи в учебном центре	обеспечение трудовой функции (РКН устно, 22.08.2025)	договор описывает процесс и третье лицо, а передача вне функции требует согласия
Доступ иностранной компании группы к справочнику или системе	ТПД без всякой пересылки (письмо РКН № 02-11-9606, 2023)	уведомление о ТПД обновляют при смене круга стран, локализация сохраняется (РКН устно, 22.10.2025)

Спорно: письменные позиции строже устной 22.08.2025 и при передаче вовне: письмо Управления РКН по Курской области от 18.06.2026 № 2467-02/46 требует согласия каждого работника при поручении подрядчику

Право на документы общества зависит от статуса, а не от наличия ПД

Кто вправе требовать документы общества с ПД работников и контрагентов и где проходит предел этого права

Privacy Advocates

КТО ЗАПРАШИВАЕТ	ОБЪЕМ ПРАВА	ПРЕДЕЛ
Участник ООО	любые документы общества (ст.8 и 50 закона об ООО), устав задает порядок, но не перечень (п.3 письма ВАС № 144)	статус на день обращения, при расхождении со списком участников по ЕГРЮЛ
Акционер	перечень п.1 ст.91 открыт всем, документы п.2 ст.91 с 1% акций, бухгалтерский учет с 25%	ниже 25% для пп.2 и 3 ст.91 нужна разумная деловая цель, период владения отсекает часть запроса
Член коллегиального органа	самостоятельное право (п.4 ст.65.3 ГК), суды применяют ст.91 по аналогии	за период до избрания только с обоснованием необходимости
Бывший участник, бенефициар, контролирующее лицо	по общему правилу нет	бывшему сведения для расчета доли или выкупа (Обобщение ВС от 15.11.2023, п.4), бенефициару при утрате контроля спорно (п.7)
Арбитражный управляющий	сведения о должнике, органах и контрагентах вне корпоративного режима, ответ за 7 дней (ст.20.3 закона о банкротстве)	переписку только через суд, отказ по мотиву 152-ФЗ суд счел поводом для дела по ч.4 ст.14.13 КоАП (А41-10789/2018)

Основание: выдача участнику закрыта п.2 ч.1 ст.6 152-ФЗ без согласия работников и контрагентов, если сведения нужны для защиты его прав (п.15 информационного письма ВАС от 18.01.2011 № 144)

Из выдаваемого участнику документа ПД не вымарывают

Порядок выдачи документа с ПД: тайны изымают, ПД оставляют, разглашение ограничивают соглашением

Privacy Advocates

1 **Статус**

на день обращения: участник ООО по списку и ЕГРЮЛ, акционер по выписке из реестра или со счета депо

2 **Объем и период**

по форме общества, доле и категории документа, для АО по справке о периоде владения

3 **Разметка**

обычная информация, конфиденциальная информация общества, охраняемая тайна, ПД третьих лиц

4 **Выдача**

обычное сразу, конфиденциальное после соглашения, тайну выпиской с изъятием, ПД при доказанной необходимости

5 **Форма**

выбирает запрашивающий: ознакомление, заверенные копии или сведения о содержании, выдачу фиксируют описью

Нельзя

- вымарывать ПД: п.7.5 указания № 7199-У касается тайн, в деле А43-1536/2016 (указание 3388-У) устояло предписание выдать договор директора без изъятий
- по экспертному подходу ссылаться на риск канала передачи как на основание отказа
- давать учетную запись вместо копий (п.13 Обобщения ВС), хотя просмотр клиент-банка присужден однажды (А41-81863/2022), спорно

vs

Можно

- потребовать соглашение о нераспространении до выдачи (п.5 ст.50 закона об ООО)
- выдать с предупреждением о запрете разглашения (п.4 ст.65.2 ГК)
- отказать в документах с ПД работников, если необходимость не доказана (Обобщение ВС от 15.11.2023, п.12), роль ст.88 ТК спорна

Данные связанных лиц собирают по норме, а не впрок

Реестры, заинтересованность, конфликт интересов, судимость и заверения: где обязанность, а где риск

Privacy Advocates

Реестр открыт не целиком

ФИО и ИНН учредителей и руководителя открыты по закону, паспортные данные выдают только госорганам, фондам, судам и АСВ (ст.6 закона о госрегистрации)

Руководитель в двух ролях

он орган общества и субъект ПД, договор за его подписью контрагент обрабатывает без согласия (РКН устно, 22.08.2025)

Сделка с заинтересованностью тянет родственников

сведения о супругах, родителях, детях, братьях и сестрах должностных лиц в составе п.1 ст.81 закона об АО и п.1 ст.45 закона об ООО

Судимость только по перечню должностей

например по ст.11.1 закона о банках, согласие проверяемого случая ч.3 ст.10 152-ФЗ не создает

КОНФЛИКТ ИНТЕРЕСОВ

родственников в объеме антикоррупционного закона обрабатывают по п.2 ч.1 ст.6 (письмо РКН от 24.12.2025 № 08-657776), сверх него с их согласия (РКН устно, 22.08.2025, 14.08.2026). Обязанность коммерческой организации спорна

СТ.431.2 ГК И ППВС № 49

Заверения вместо истребования

примеры в п.34 ППВС от 25.12.2018 № 49: структура контроля, отсутствие крупности и конфликта интересов руководителя

Рекомендация: по экспертному подходу родственные связи руководства держат вне общей кадровой системы, а о доходах запрашивают третьих лиц только по норме (письмо РКН от 15.03.2022 № 08-16351 о госслужащих)

Передача ПД держится на цели, верном документе и контроле цепочки

Выводы раздела

Privacy Advocates

01

Цель решает роль

нет своей цели - обработчик, своя цель и отношения с субъектом - самостоятельный оператор, а статус считают по каждому потоку

02

Доступ решает поручение

облако, хостинг и обслуживание квалифицируют по доступу к содержанию, а Роскомнадзор - и без доступа

03

Поручение предметно

перечень действий, меры, аудит, сжатые сроки по инцидентам и уничтожение с подтверждением

04

Между операторами - DTA

основание передачи, взаимные заверения и одиннадцать блоков вместо обычного NDA

05

Проверка до доступа

чек-лист по типу передачи, обязательные критерии и пересмотр раз в 3 года

06

Цепочка до последнего звена

субобработчики, компании группы и доступы бывших подрядчиков учитывают так же, как прямые передачи

ЧАСТЬ

VI

Цифровая среда и ИИ

Сайты, авторизация, ИИ и синтетический контент

22 Комплаенс ПД на сайте
23 Авторизация пользователей
24 Искусственный интеллект и ПД
25 Дипфейки

22

Комплаенс ПД на сайте

Как РКН проверяет сайты и что исправить заранее

22.1 Как Роскомнадзор проверяет сайты

22.2 Зоны контроля на сайте

Раздел на сайте
privacy-advocates.ru/pd/saj

22.1

Как Роскомнадзор проверяет сайты

- Сайт проверяют от внешнего осмотра к разбору 12 зон
- Диагностика комплаенса ПД на сайте
- АС МПД сама находит сайты и ранжирует нарушения
- Признаки нарушений находят на большинстве проверенных сайтов

Сайт проверяют от внешнего осмотра к разбору 12 зон

Схема диагностики комплаенса ПД на сайте: имитация проверки Роскомнадзора и детальный разбор

Privacy Advocates

01

ЭТАП 1

Имитация проверки Роскомнадзором

внешний осмотр без взаимодействия с оператором: страницы, формы, документы, домен, хостинг, cookie, сверка с реестром. Затем по каждой зоне фиксируют разрыв и меру исправления

ЭТАП 2. ДВЕНАДЦАТЬ ЗОН КОНТРОЛЯ КОМПЛАЕНСА ПД НА САЙТЕ

1. эпизоды сбора ПД в формах и компонентах страниц
2. ответственное лицо: домен, ресурс, оператор
3. локализация баз с ПД граждан РФ
4. внешние сервисы: поручение или иная модель
5. договор с пользователями: соглашение, оферта, согласие
6. фиксация юридически значимых действий
7. мониторинг и аналитика поведения пользователей
8. маркетинговые и информационные рассылки
9. публикация ПД с согласия на распространение
10. уведомления об обработке и о трансграничной передаче
11. информирование о рекомендательных технологиях
12. авторизация пользователей

Совет: осмотр, который оператор проводит сам раз в квартал, воспроизводит ту картину сайта, которую Роскомнадзор видит снаружи

Диагностика комплаенса ПД на сайте

Типовые нарушения в четырех областях контроля и их критичность

Privacy Advocates

Локализация и трансграничная передача

- сбор ПД в БД на иностранном хостинге
- сбор ПД иностранными метриками и сервисами (Google Analytics, reCAPTCHA)
- ТПД не указана в политике и согласиях

Согласия и соглашения

- нет согласия на прямой маркетинг и (или) рекламу
- нет согласия на распространение ПД
- нет информирования о метриках при входе на ресурс
- согласие без отдельного волеизъявления
- бездействие пользователя как условие согласия

Политика

- нет ссылки на политику на страницах сбора ПД
- веб-формы сбора ПД расходятся с политикой
- не описаны сторонние метрики и сервисы
- не описана обработка по целям и уничтожение ПД
- не указан срок (условие) прекращения обработки

Уведомления, рекомендации и авторизация

- не поданы уведомления об обработке и (или) ТПД
- обработка расходится с поданными уведомлениями
- избыточность собираемых ПД по отношению к целям
- нет правил рекомендательных технологий (ст.13.56)
- иностранные сервисы входа (ст.13.55)

Критичность контроля высокая средняя умеренная

АС МПД сама находит сайты и ранжирует нарушения

Система мониторинга прав субъектов ПД в интернете: функции, нарушения, приоритетные сферы

Privacy Advocates

РАНЖИРОВАНИЕ НАРУШЕНИЙ

1. нет согласия на обработку
2. нет политики обработки ПД
3. форма шире политики
4. ссылки на чужие формы сбора
5. сбор ПД россиян на зарубежном хостинге
6. в политике нет сведений о ТПД
7. метрика не указана в политике
8. нет или неверен срок обработки
9. нет уведомления об обработке

ФУНКЦИИ СИСТЕМЫ

- поиск ресурсов, где собирают и распространяют ПД
- проверка по жалобам и плану мероприятий
- интеграция с формой обращений граждан
- не менее **500 тыс.** ресурсов в год и **15 тыс.** в неделю по словам "согласие", "продам базу"
- модуль доказательной базы

Приоритет мониторинга: **банки, НПФ, МФО, платежные**; страховщики; **коллекторы**; соцсети; связь; **интернет-магазины**; транспорт; почта; медицина; **образование**; **ЖКХ и УК**; МФЦ; **органы власти**

Следствие: система сверяет согласия и политики с полями форм и сведениями ЕГРЮЛ, поэтому расхождение документов с фактическим сбором видно без участия оператора

Признаки нарушений находят на большинстве проверенных сайтов

Практика автоматизированного дистанционного контроля Роскомнадзора 2024-2026

Privacy Advocates

2024

ИТОГИ ГОДА

77% с признаками нарушений

около 6,5 тыс. требований о приведении сайта в соответствие, 258 протоколов

1 пол. 2025

ПОЛУГОДИЕ

почти 27 тыс. проверок

признаки нарушений в 84% случаев, 8 тыс. требований, 208 протоколов

2026

14.08.2026

почти 160 тыс. ресурсов

охват удвоился против 80 тыс. годом ранее, признаки нарушений почти в 90% случаев

9 из 10

срабатываний верны

по словам Роскомнадзора, ошибается примерно каждое десятое, отдельной процедуры оспаривания машинной оценки нет

единицы %

злостных нарушителей

протокол Роскомнадзор называет крайней мерой при отсутствии отклика на требование

ОТБОР

Кого проверяют первыми

сферы, на которые больше всего жалуются граждане: финансовый сектор, интернет-магазины, образование, ЖКХ

- по ТЗ 2021 года в выборку попадают сайты, собирающие или распространяющие ПД, сайты по жалобам и сайты из плана наблюдения

Имитация проверки охватывает четыре зоны сразу

Типовые нарушения по зонам внешнего осмотра Роскомнадзора, слева направо от более критичных

Privacy Advocates

	критичнее				менее критично
Локализация и ТПД	база ПД на иностранном хостинге	иностранные метрики и формы: Google Analytics, reCAPTCHA	ТПД не указана в политике, согласиях и соглашениях		
Согласия и соглашения	нет согласия на маркетинг и рекламу	нет согласия на распространение	нет информирования о метриках при входе	согласие без отдельного волеизъявления	бездействие пользователя как условие согласия
Политика	нет ссылки на политику на страницах сбора	формы не совпадают с описанием в политике	не описаны сторонние метрики, формы и сервисы	нет описания по целям и порядка уничтожения	нет или неверен срок прекращения обработки
Уведомления, рекомендации, авторизация	не поданы уведомления об обработке и ТПД	обработка расходится с уведомлением	избыточный сбор по отношению к целям	нет ссылки на правила рекомендательных технологий	иностранные сервисы авторизации (SSO)

Пример: требование Управления Роскомнадзора по ЮФО от 11.02.2025 по одному сайту: чекбокс ознакомления с политикой вместо согласия, Google Analytics как признак нарушения ч.5 ст.18, нет уведомления о трансграничной передаче, в политике нет категорий, сроков и порядка уничтожения по целям

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OTV-003	Ландшафт юридической ответственности за ПД	30 Ответственность

22.2

Зоны контроля на сайте

- Для каждого вида взаимодействия на сайте нужен свой документ
- Администратор домена - оператор, пока не доказано иное
- Собирать ПД россиян в зарубежные базы нельзя
- Поручение нужно инфраструктуре сайта, а не каждому виджету

Для каждого вида взаимодействия на сайте нужен свой документ

Три блока отношений с пользователем, способы взаимодействия и документы, которые их оформляют

Privacy Advocates

БЛОК ВЗАИМООТНОШЕНИЙ	СПОСОБЫ ВЗАИМОДЕЙСТВИЯ	ДОКУМЕНТЫ, КОТОРЫЕ ОФОРМЛЯЮТ ОТНОШЕНИЯ
Функционал и контент ресурса	просмотр страниц, чекбокс, пароль, ввод данных, онлайн-чат	пользовательское соглашение (Terms of Use), политика конфиденциальности сайта (Online Privacy Policy), ссылка внизу сайта на политику обработки ПД компании (Data Processing Policy)
Аналитика, маркетинг и рассылки	всплывающее сообщение, чекбокс single opt-in, PIN-код или ссылка для double opt-in	уведомление о файлах cookie (Cookie Notice), согласие на маркетинг и информационные рассылки (Marketing Consent)
Отдельные бизнес-активности	покупка, ввод данных, загрузка файлов	публичная оферта или договор присоединения с уведомлением о конфиденциальности (Privacy Notice), согласие на обработку ПД (Personal Data Processing Consent)

ТИПЫ COOKIE ПО ABOUTCOOKIES.COM

Critical: необходимые | **Functional: предпочтения** | **Analytical: статистика** | **Marketing: реклама и таргетинг** | **Social: соцсети**

Ловушка: реестр по формам ввода покрывает только то, что вводит пользователь. Сведения из cookie и метрик и производные профили выпадают из документов и всплывают при осмотре страницы

Администратор домена - оператор, пока не доказано иное

Как надзор и суд определяют лицо, ответственное за обработку ПД на сайте

Privacy Advocates

Администратор домена

лицо, на имя которого зарегистрировано доменное имя для сетевой адресации

Владелец сайта

лицо, которое самостоятельно и по своему усмотрению определяет порядок использования сайта, в том числе размещения информации

Оператор ПД

лицо, которое организует или осуществляет обработку и определяет ее цели, состав ПД и действия с ними

ЛОГИКА НАДЗОРА И СУДА

администратор домена = владелец сайта = оператор ПД

пока не доказано обратное, а опровергать презумпцию приходится самому оператору

ЧЬИ ПРАВА ВЫЯСНЯЕТ НАДЗОР

- доменное имя
- дизайн и контент
- CMS и базы данных
- ИТ-инфраструктура

Практика: в деле о блокировке LinkedIn Мосгорсуд (33-38783/16, 10.11.2016) оставил в силе решение: за содержание сайта отвечает администратор домена, поскольку без его контроля ресурс использовать нельзя. Если оператором должен быть другой, права раскладывают договорами заранее

Собирать ПД россиян в зарубежные базы нельзя

Ч.5 ст.18 152-ФЗ в редакции 23-ФЗ с 01.07.2025: когда нужна локализация и как ее оценивают

Privacy Advocates

Ч.5 СТ.18 152-ФЗ С 01.07.2025

при сборе ПД, в том числе через интернет, запись, систематизация, накопление, хранение, уточнение и извлечение ПД граждан РФ с использованием баз за рубежом **не допускаются**, кроме случаев пп.2, 3, 4, 8 ч.1 ст.6

ВОПРОС	ЛОКАЛИЗАЦИЯ НУЖНА	НЕ НУЖНА
Чьи ПД	граждан РФ, база направлена на РФ	иных лиц
Источник ПД	субъект, открытые источники, мониторинг поведения, правка в базе	только другие базы
Основание	любое, кроме исключений	пп.2, 3, 4, 8 ч.1 ст.6
Где база	за рубежом	в России

Метрики

управления Роскомнадзора по ПФО, Курганской области и ЮФО считали Google Analytics нарушением ч.5 ст.18, центральный аппарат (04.08.2025) и Минцифры (12.05.2025) видят в нем ТПД

Направленность на РФ

домен .ru, .рф, .su, русский интерфейс, услуги в РФ. Штраф Ookla 6 млн ₽ устоял в кассации (16-1536/2025): регистрация открыта. По Taobao апелляция 29.09.2026 (А40-325054/2025) отвергла и запрет регистрации при доступе из России

Выводы: не держать собранные в РФ ПД в зарубежных базах. Данные, полученные анализом ранее собранного в России массива, можно обрабатывать за рубежом

Поручение нужно инфраструктуре сайта, а не каждому виджету

Как оформлять внешние сервисы: поручение обработки или работа без поручения

Privacy Advocates

По мнению Роскомнадзора, поручение возникает, когда оператор **способен сам** провести обработку, включая доступ и хранение, но **решил делегировать** ее полностью или частично контрагенту-обработчику

НУЖНО ПОРУЧЕНИЕ ОБРАБОТКИ

- виртуальный хостинг
- облачные сервисы SaaS, PaaS, IaaS
- администрирование и поддержка
- ИТ-безопасность
- IaaS не всегда поручение: позиция RPPA

БЕЗ ПОРУЧЕНИЯ: СЕРВИС ОКАЗЫВАЕТ УСЛУГУ ПОЛЬЗОВАТЕЛЮ ИЛИ ОПЕРАТОРУ

- SSO: Яндекс ID, VK ID, Сбер ID, ЕСИА
- вход: LastPass, OneLogin
- формы: Google Forms, Яндекс Формы
- чаты: Chatra, Jivosite
- опросы: Typeform, Анкетолог
- оплата: Mastercard API, PayPal
- виджеты: VK, Яндекс
- медиа: YouTube, Vimeo
- защита: reCAPTCHA, Cloudflare
- аналитика: Google Analytics, Метрика
- карты: Google, Яндекс
- шрифты: Google Fonts
- почта: MailGun
- ЭП: SignNow, Диадок
- согласия: OneTrust
- отзывы: Foursquare, Yelp
- Search Console

Риск: иностранный сервис из любой группы означает ТПД и риск нелокализации. По позиции Роскомнадзора 14.08.2026 положение о ТПД включают и в пользовательское соглашение, и в политику

Согласие отделяют от политики и пользовательского соглашения

Политика и согласие по рекомендациям Роскомнадзора, договор с пользователем и статус посредника

Privacy Advocates

Политика конфиденциальности

рекомендации Роскомнадзора по содержанию

- сведения об операторе
- цели, категории и перечень ПД, категории субъектов, способы, сроки обработки и хранения, порядок уничтожения (п.2 ч.1 ст.18.1)
- правовые основания и меры по выполнению 152-ФЗ
- способы связи с оператором
- при наличии: передача третьим лицам и трансграничная передача

Согласие на обработку ПД

конкретное, предметное, информированное, сознательное, однозначное

- сведения об операторе
- цели, категории и перечень ПД, категории субъектов, способы, сроки, порядок уничтожения
- способы связи, в том числе для отзыва согласия
- ссылка на политику оператора
- при наличии: передача третьим лицам и трансграничная передача

Обособление

не всякую обработку легализует договор, тогда согласие дают отдельным текстом, визуально и по смыслу обособленным, отдельным волеизъявлением

Browse-wrap

плашки "продолжая использовать сайт, вы соглашаетесь" мало: молчание не акцепт (п.2 ст.438 ГК), а Роскомнадзор устно (31.01.2024) требует перехода по ссылке на полный текст с записью в журнале

Посредник

сайт без статуса СМИ или соцсети с аудиторией свыше 500 тыс. в сутки (ст.10.6 149-ФЗ) не отвечает за чужой контент, пока не узнал о нарушении (18-П от 09.07.2013, А40-236948/2025)

Клик по кнопке доказывают журналом действий пользователя

Click-wrap, журнал юридически значимых действий и судьба законопроекта о подтверждении кодом

Privacy Advocates

1

Текст и условия

пользователь видит текст договора или согласия и описание условий

2

Клик "Подтверждаю"

click-wrap: договор или согласие заключают щелчком по клавише "я согласен" рядом с текстом

3

Запись в журнал

access_log фиксирует IP-адрес, дату и время, страницу и браузер пользователя

4

Хранение журнала

журнал защищают и хранят как доказательство юридически значимого действия

ЧТО УЧЕСТЬ ПРИ ЛОГИРОВАНИИ

1. требований к составу и сроку хранения логов нет, поэтому соблюдают минимизацию данных
2. обеспечивают конфиденциальность, целостность и доступность журналов
3. запись логов может быть сбором ПД, поэтому журналы лучше вести на локализованных в РФ ресурсах

ЗАКОНОПРОЕКТ 2026 ГОДА

Код подтверждения не стал обязанностью

обсуждалось подтверждение значимых действий кодом по СМС и в мессенджере Max с 01.09.2026, но в принятый 26.06.2026 второй антифрод-пакет (210-ФЗ) норма не вошла

Учесть: простая веб-форма согласия без последующей идентификации пользователя дает среднюю степень вреда по приказу Роскомнадзора № 178

Роскомнадзор: метрики включают после согласия, одной политики мало

Cookie-баннер, описание файлов cookie и требования Роскомнадзора к метрическим программам

Privacy Advocates

Роскомнадзор: если на сайте работают метрики, оператор должен

- сообщить пользователю при входе на сайт о метрических программах и получить согласие на обработку ПД, собираемых ими
- указать, какие именно программы используются
- включить в политику конфиденциальности сведения о метрических программах

Ссылки на политику мало: условия согласия описывают в отдельном файле или разделе, а согласие обособляют от иных документов

ПРИМЕР ОПИСАНИЯ COOKIE В ПОЛИТИКЕ

ТИП	ВЛАДЕЛЕЦ	ЦЕЛЬ	СРОК	КАК ОТКЛЮЧИТЬ
Технические	оператор	работа сайта, безопасность, вход	удаляются через месяц после визита	в настройках браузера, вход станет неудобнее
Аналитика	Google Analytics	статистика посещений и улучшение сайта	до закрытия браузера или до 24 месяцев	на странице отказа от отслеживания Google

Нюансы: технические cookie без идентификации посетителя Роскомнадзор устно (27.08.2025) к ПД не относит, метрические относит. На дне открытых дверей 14.08.2026 вход на сайт после информирования назван согласием, письменные разъяснения требуют активного действия, поэтому безопаснее кнопка. Анонимизация IP в Google Analytics не спасает: cookie и данные устройства уходят открыто

Удаленный осмотр сайта ведет к требованиям и делам по ст.13.11

Требования управлений Роскомнадзора 2026 года и прокурорская проверка сайтов учреждений Коломны

Privacy Advocates

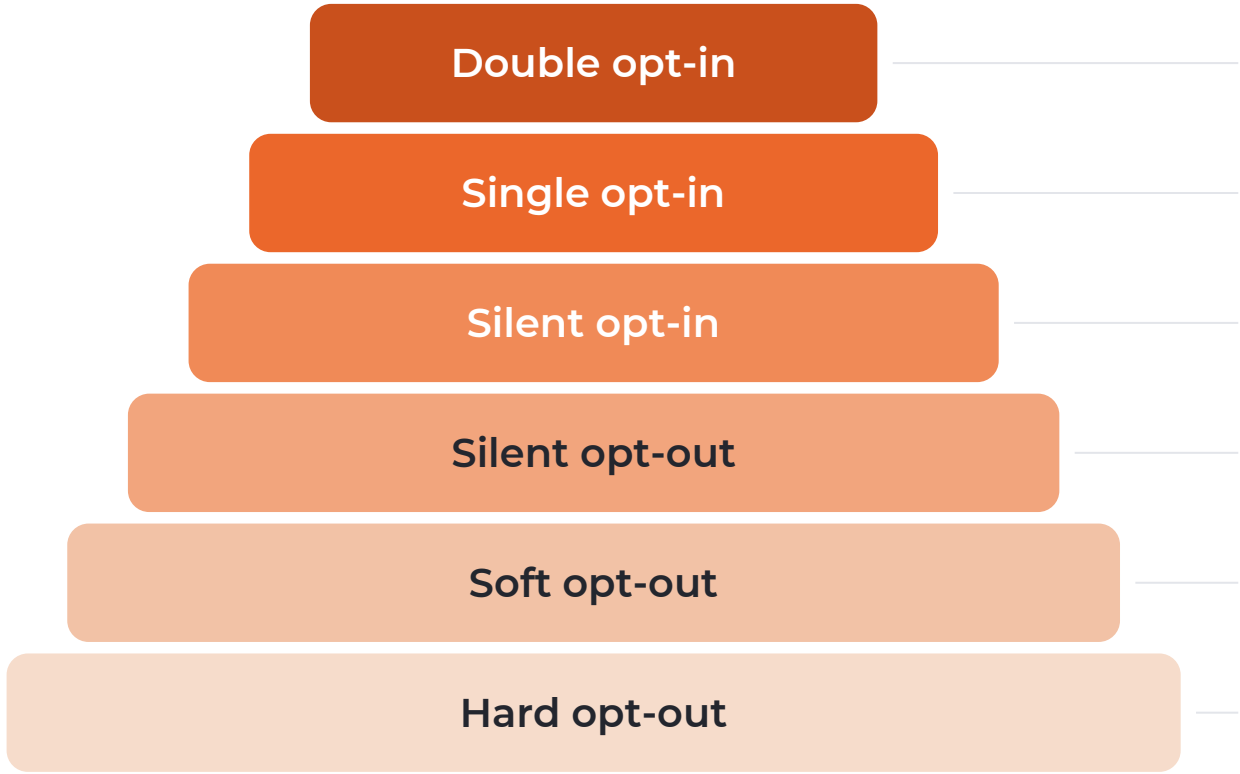
КТО	ЧТО ВЫЯВЛЕНО	ИСХОД
Роскомнадзор, Тюмень, ХМАО и ЯНАО, 24.07.2026	метрика без основания и информирования, нет срока в договоре с пользователем, дефекты политики, нет уведомления	привести обработку в соответствие
Роскомнадзор по ЦФО, 19.08.2026	метрические программы без основания, избыточный и неустановленный срок в политике	**прекратить обработку с нарушением**
Прокурор, музей-заповедник, 10.06.2026	Метрика без предупреждения о cookie и согласия (ч.1), политика не охватывает метрические данные (ч.3)	два предупреждения директору (5-361/2026, 5-362/2026)
Прокурор, учреждение, 16.06-31.08.2026	те же нарушения на сайте учреждения	150 тыс. ₽ отменено, при новом рассмотрении предупреждение по просьбе (5-349/2026)

Вывод: все позиции видны снаружи: политика, договор с пользователем, счетчики и реестр операторов. Самопроверку сайта ведут по полному составу требований, а не только по интерфейсу

Чем пассивнее согласие на рассылку, тем выше риск

Механизмы подписки от double opt-in до hard opt-out и ориентиры ФАС и Банка России

Privacy Advocates



- **Double opt-in** — согласие дважды: отметка в форме и подтверждение по ссылке из письма
- **Single opt-in** — согласие один раз: отметка в пустом чекбоксе "Согласен на обработку ПД"
- **Silent opt-in** — отметка уже стоит и ее не сняли, или кнопка "Отправить" с оговоркой о согласии
- **Silent opt-out** — предустановленное несогласие: отметка "Не согласен" уже стоит
- **Soft opt-out** — отказ через отрицание: "Не согласен" или двойное "Не согласен с отказом"
- **Hard opt-out** — согласие вшито в новые условия и считается данным, если не прислан отказ

Практика: по словам Роскомнадзора 14.08.2026 крупные операторы чаще всего нарушают ч.1 ст.15 152-ФЗ именно на почтовых рассылках. Отписка от рассылки отзывом согласия не является, это разные элементы интерфейса. Отдельно соблюдают регулирование массовых и автоматических вызовов

Темные паттерны выдают любое действие за согласие

Формулы, которыми интерфейсы получают согласие без настоящего выбора

Privacy Advocates

УЗНАЕТЕ ЭТИ ФОРМУЛЫ?

- нажимая "Отказаться", "Сбросить звонок", "Выйти" или "Закрыть", вы соглашаетесь на обработку ваших данных...
- используя банкомат так, что он считывает параметры вашего лица, вы соглашаетесь...
- не ответив на три звонка поддержки банка, вы соглашаетесь...
- удаляя или скачивая приложение банка, вы соглашаетесь...
- оплачивая покупки картой банка, вы соглашаетесь...
- отзывая согласие, вы соглашаетесь...

ШУТКА С ДОЛЕЙ ПРАВДЫ

Согласие одним "спасибо"

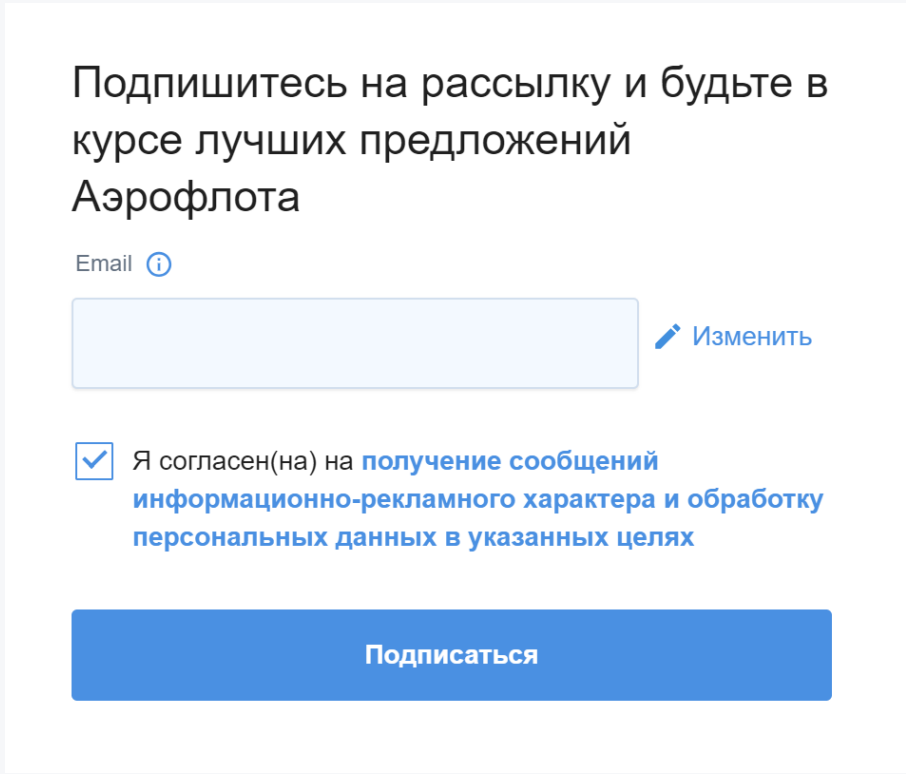
Поддержка банка сообщает клиенту, что согласия на биометрию он не давал. Клиент отвечает "Спасибо", ассистент присылает жест "окей", а мелким шрифтом на жесте: нажав "Спасибо", вы соглашаетесь

- согласие должно быть среди прочего конкретным, информированным, сознательным и однозначным (ч.1 ст.9)
- отказ не должен быть сложнее согласия

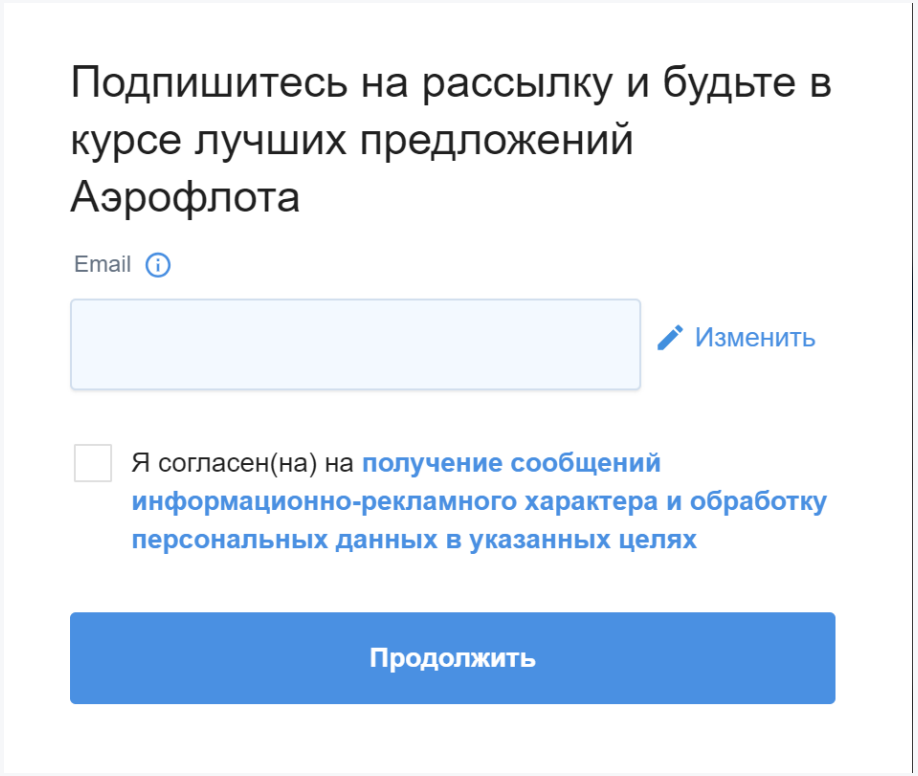
Окно подписки без крестика - это темный паттерн

Пример с сайта авиакомпании: закрыть окно можно, только сняв заранее поставленную галочку

Privacy Advocates



Крестика нет, галочка согласия уже стоит



Чтобы закрыть окно, нужно снять галочку и нажать "Продолжить"

Вывод: предустановленная галочка - пассивное согласие (silent opt-in): оно не конкретное и не однозначное, а отказ сложнее согласия. Такие окна в своих продуктах лучше не делать

Публикация ПД на сайте требует согласия на распространение

С 01.03.2021 публикация ПД на открытых страницах требует согласия по ст.10.1 152-ФЗ

Privacy Advocates

Сервис Роскомнадзора

pd.rkn.gov.ru/soglasiya: рекомендации по подготовке согласия на распространение

Образец согласия RPPA

rppa.ru/_media/analitika/srpd.docx

> Размещенные на этой странице персональные данные распространяются с разрешения субъекта для цели [...]. Субъектом установлены следующие условия и запреты на обработку таких данных любыми лицами: [...]

Дисклеймер рядом с опубликованными ПД по ч.10 ст.10.1 152-ФЗ, не позднее трех рабочих дней после получения согласия

Спорно: согласие по ст.10.1 - частный случай согласия по п.1 ч.1 ст.6, распространять можно и по иным основаниям: АС Московского округа 30.03.2023, ВС отказал в передаче жалобы 21.07.2023 (А40-139096/2022), письмо Роскомнадзора от 15.05.2024 № 08-166301. Устные позиции 2025-2026 годов строже

Об обработке и о ТПД уведомляют раздельно и заранее

Что изменилось с 01.09.2022 и 01.03.2023 и формы уведомлений по приказу Роскомнадзора № 180

Privacy Advocates

Обработка ПД, ст.22

С 01.09.2022 уведомлять нужно и в прежних исключениях

- ПД работников и соискателей по ТК РФ
- ПД для заключения и исполнения договора с субъектом
- ПД членов общественных объединений и религиозных организаций
- ПД, распространяемые с согласия субъекта
- только ФИО или обработка для пропуска на территорию
- ПД в ИСПД, поименованных в федеральных законах

Трансграничная передача, ч.3 ст.12

Отдельное уведомление о намерении до начала ТПД

- подают отдельно от уведомления по ст.22 и указывают его реквизиты
- кто вел ТПД до 01.03.2023, направил уведомление и сведения о правовых основаниях по ст.6
- письменное согласие субъекта для этого не нужно, деятельность на время рассмотрения не приостанавливают
- Роскомнадзор вправе за 10 рабочих дней запретить или ограничить передачу
- в страны вне перечня адекватных передавать до истечения срока рассмотрения нельзя

Практика: при дистанционном осмотре сайта Роскомнадзор сверяет его с реестром операторов, и отсутствие уведомления становится отдельным пунктом требования наравне с дефектами сайта

Рекомендательные технологии требуют правил и уведомления

Ст.10.2-2 149-ФЗ: кого касается, исключения и две обязанности, которые чаще всего путают

Privacy Advocates

ЧТО РЕГУЛИРУЕТСЯ

Рекомендательные технологии

информационные технологии предоставления информации на основе сбора, систематизации и анализа сведений о предпочтениях пользователей, находящихся в России

Кого касается

владельцев сайтов, приложений, систем и программ - граждан РФ и российских юрлиц, выдающих информацию по предпочтениям пользователей в России

Не распространяется

на операторов ГИС, госорганы и органы местного самоуправления, а также на выдачу по заданным пользователем параметрам и фильтрам

Схема рекомендательных технологий

скачать

Правила применения

- процессы и методы сбора и анализа сведений о предпочтениях, способы их осуществления, виды и источники сведений
- русский язык, доступ без оплаты, регистрации и идентификации, текст ничем не перекрыт

Уведомление о применении

- на всех страницах, включая персональные: "На информационном ресурсе применяются рекомендательные технологии"
- ссылка на отдельную страницу с дословно заданным текстом о сборе и анализе предпочтений

Запрет: нельзя применять технологии, нарушающие права или выдающие информацию с нарушением закона. С 07.07.2026 действует ст.13.56 КоАП, ЮЛ 500-700 тыс. ₽, повторно 1-1,4 млн ₽, за неисполнение требования до 2,8 млн ₽

619

Пользователей в России авторизуют только четырьмя способами

Ч.10 ст.8 149-ФЗ: обязанность с 01.12.2023, санкция ст.13.55 КоАП с 07.07.2026

Privacy Advocates

1. **Номер мобильного телефона**
   оператор связи может быть нероссийским: прямого запрета в законе нет
2. **ЕСИА**
   вход через портал госуслуг
3. **ЕБС**
   вход через единую биометрическую систему
4. **Иная система входа**
   владелец - гражданин РФ без иного гражданства или российское юрлицо: собственный вход, VK ID, Яндекс ID

КОГО КАСАЕТСЯ

Российские владельцы ресурсов с доступом для авторизованных

критерий - нахождение пользователя в России, а не гражданство, иностранные ресурсы иностранных владельцев вне нормы. Понятие авторизации закон не раскрывает, поэтому проверяют регистрацию и повторные входы

Запрещено
иностранные сервисы входа: Apple ID, Google Sign-In, вход через Telegram

Допустимо
иностранная почта как идентификатор и канал доставки кода. Ввод почты при регистрации Роскомнадзор авторизацией не считает (письмо от 11.06.2026)

Законопроект
поправка о праве Правительства установить случаи входа по почте в российской доменной зоне в закон не вошла

С 07.07.2026: за нарушение правил авторизации юрлицам грозит штраф от 500 до 700 тыс. ₽ (ст.13.55 КоАП, 199-ФЗ от 26.06.2026)

23

Авторизация пользователей

Особенности и перспективы регулирования на российских сайтах, в приложениях и системах

23.1 Регулирование авторизации

23.2 Требования и ответственность

23.3 Практика и вопросы

23.4 Антифрод-3

Раздел на сайте
privacy-advocates.ru/pd/avt

23.1

Регулирование авторизации

- Регулирование авторизации
- Идентификация, аутентификация, авторизация
- Что регулируется
- Правовая основа и мотив

Регулирование авторизации

Обязанность авторизовать российских пользователей одним из разрешенных способов

Privacy Advocates

01

Что регулируется

Авторизация пользователей сайтов, приложений, информационных систем и ПО для доступа к их содержимому

02

Кого касается

Владельцы ресурсов, работающие на российскую аудиторию, - для пользователей, находящихся в РФ

03

Требования

Авторизация одним из четырех способов и запрет иностранных сервисов входа - Apple ID, Google Sign-In

04

Чем регулируется

ч.10 ст.8 149-ФЗ "Об информации" в редакции 406-ФЗ от 31.07.2023

05

Ответственность

Административная (КоАП) и уголовная (УК) - за неисполнение и за передачу данных авторизации

06

Перспективы

Антифрод-3: расширение круга обязанных лиц, абонентский номер как идентификатор и хранение сведений о входах

Идентификация, аутентификация, авторизация

Общепринятые технические понятия и особый смысл термина в ч.10 ст.8 149-ФЗ

Privacy Advocates

149-ФЗ эти термины не раскрывает. Их общепринятое значение задает ГОСТ Р 58833-2020 "Защита информации. Идентификация и аутентификация. Общие положения" - три самостоятельные процедуры, следующие одна за другой.

Идентификация

"Кто это?"

Пользователь предъявляет идентификатор - логин, адрес почты, номер телефона, - а система сравнивает его с перечнем присвоенных.

Аутентификация

"Он ли это?"

Система проверяет подлинность пользователя и то, что предъявленный идентификатор принадлежит именно ему - пароль, код из SMS, биометрия, ключ доступа.

Авторизация

"Что ему можно?"

Система предоставляет права доступа или иные полномочия по установленным правилам. Успешное опознание пользователя - лишь одно из оснований для этого.

В ч.10 ст.8 149-ФЗ "авторизация" - это не предоставление прав доступа

Норма говорит о доступе для пользователей, прошедших авторизацию, и требует проводить ее одним из четырех способов - абонентский номер, ЕСИА, ЕБС, иная информационная система. По ГОСТ все это средства идентификации и аутентификации, а не предоставления прав. Поэтому "авторизация" закона ближе к тому, что в технике называют "входом".

Что регулируется

Авторизация как условие доступа к информации на ресурсе

Privacy Advocates



ПРЕДМЕТ РЕГУЛИРОВАНИЯ

Авторизация пользователей сайтов, мобильных приложений, информационных систем и программного обеспечения, необходимая для предоставления доступа к размещенной на них информации.



Широкий охват

Требование способно затронуть операционные системы и прикладное ПО (например, Microsoft Office), публичные точки Wi-Fi и мобильные устройства - везде, где разграничен доступ к информации.



Понятие не определено

Термин "авторизация" закон не раскрывает, а авторы законопроекта говорят о "регистрации". До официальных разъяснений требование может охватывать и первичный вход, и дальнейшее использование ресурса.

Правовая основа и мотив

Что вводит требование и как его объясняют авторы

Privacy Advocates

Чем регулируется

ДЕЙСТВУЮЩАЯ НОРМА

ч.10 ст.8 149-ФЗ

Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006.

Требование введено 406-ФЗ от 31.07.2023

Декларируемый мотив

"Закон направлен на защиту персональных данных наших граждан, с учетом того, что многие иностранные сервисы явно или неявно участвуют в информационной войне".

Автор законопроекта

Кого касается

Привязка не к гражданству, а к местонахождению пользователя

Privacy Advocates

Владельцы ресурсов - российские компании и физлица, открывающие доступ только "авторизованным" пользователям и работающие на территории РФ.

Пользователи в РФ

Авторизация нужна для тех, кто находится на территории РФ. Иностранные граждане в РФ подпадают под требование наравне с россиянами.

Пользователи за рубежом

Находящиеся за пределами РФ (включая россиян за границей) формально не подпадают - для них можно сохранить вход через иностранные SSO.

Как определяют место

Порядок не установлен: на практике смотрят на IP, геолокацию, код страны номера (+7). VPN размывает критерий и создает риск ошибки в обе стороны.

Критерий "деятельность в сети Интернет на территории РФ" не раскрыт. По аналогии с 236-ФЗ на российскую аудиторию указывают русскоязычный интерфейс, реклама для РФ, домены в российских зонах, расчеты в рублях.

На кого не распространяется

Изъятия из требования и отсутствие обратной силы

Privacy Advocates

Иностранные ресурсы

Если владелец - иностранный гражданин или организация, вход через Google, Apple и любые другие SSO можно сохранить.

Иностранная электронная почта

Адреса иностранных почт остаются допустимыми идентификаторами: "системой, обеспечивающей авторизацию", считается ПО самого российского ресурса.

Регистрация до 01.12.2023

Обратной силы у требования нет - пользователи, зарегистрировавшиеся раньше этой даты, сохраняют доступ к ресурсам.

Важно: право Правительства РФ разрешить авторизацию по e-mail в российской доменной зоне пока не реализовано.

23.2

Требования и ответственность

- Требования: способы авторизации
- Ответственность

Требования: способы авторизации

Российских пользователей авторизуют одним из четырех способов

Privacy Advocates

01 Абонентский номер

По номеру мобильного телефона. Прямого запрета на нероссийского оператора связи в законе нет.

02 ЕСИА

Через Единую систему идентификации и аутентификации - проще говоря, с помощью портала Госуслуг.

03 ЕБС

Через Единую биометрическую систему, где хранятся биометрические данные граждан РФ.

04 Иная информационная система

Система гражданина РФ без второго гражданства или российского юрлица: своя авторизация ресурса или SSO - VK ID, Яндекс ID.

Иностранные сервисы авторизации запрещены. На российских ресурсах больше нельзя использовать Apple ID, Google Sign-In и аналоги.

Ответственность

Административные и уголовные санкции за нарушения

Privacy Advocates

КоАП РФ · СТ.13.55

Неисполнение обязанности авторизации с 07.07.2026

ЮЛ	**500-700К ₽**
ДЛ	**30-50К ₽**
ФЛ	**до 20К ₽**

КоАП РФ · СТ.13.29.2

Передача данных авторизации без согласия

ЮЛ	**до 200К ₽**
ИП	**до 100К ₽**
ФЛ	**до 50К ₽**

УК РФ · СТ.274.5

Организация передачи таких данных

Штраф	**до 700К ₽**
Лишение свободы	**до 3 лет**
Принудработы	**до 3 лет**

23.3

Практика и вопросы

- Проблематика и практика рынка
- Вопросы и ответы: границы запрета
- Вопросы и ответы: реализация
- Риск-ориентированный подход

Проблематика и практика рынка

Открытые вопросы применения и первая реакция сервисов

Privacy Advocates

Судьба учетных записей

Неясно, что произойдет с аккаунтом, если пользователь не сменил вход через иностранную SSO, а ресурс уже убрал этот способ.

Конфликт с правилами Apple

Пункт 4.8 правил App Store с 2024 года требует равноценную альтернативу входа с защитой приватности, не обязательно Sign in with Apple, поэтому прямого противоречия запрету нет.

РЫНОК УЖЕ РЕАГИРУЕТ

"Литрес" и VK Play убирают вход через Apple и Google ID; **Ozon** уже отключил такую авторизацию.

Вопросы и ответы: границы запрета

Что подпадает под ч.10 ст.8 149-ФЗ и кто отвечает за нарушение

Privacy Advocates

? Иностранная почта как логин - это уже нарушение?

Нет. Запрещена кроссавторизация, то есть кнопка входа через иностранный сервис. Адрес Gmail, введенный как логин, доступа к учетной записи не дает. Так норму читают РКН и авторы законопроекта, но часть публикаций толкует ее шире.

? Отвечает ли сам пользователь за выбор способа входа?

Нет. Субъект ст.13.55 КоАП - владелец сайта, страницы, информационной системы или программы. Штраф для граждан 10-20 тыс. ₽ адресован владельцам-физлицам, а не посетителям: риск возникает у ресурса, а не у того, кто на него зашел.

? Кто отвечает, если вход реализует платформа?

Владелец сервиса, на чьей стороне технически проходит авторизация. Если пользователи приходят уже авторизованными платформой, это ее зона ответственности. Запрос РКН может прийти и вам, поэтому нужны договор, схема входа и ответ поддержки.

? Действует ли запрет для корпоративных и B2B-сервисов?

Да. Изъятий для внутренних и корпоративных сервисов нет: вход сотрудников в таск-трекер или админ-панель через Google-аккаунт подпадает под запрет наравне с входом клиентов.

Вопросы и ответы: реализация

Местонахождение пользователя, доставка кодов и выбор системы входа

Privacy Advocates

? Как определять местонахождение пользователя?

Порядок не установлен. На практике смотрят на IP и геолокацию, реже на код страны номера, и проверяют на момент входа. Критерий - местонахождение, а не гражданство и не домен почты. Пользователя за VPN система видит как иностранного.

? Код входа приходит на Gmail или в Telegram - это нарушение?

Нет. Доставка кода или ссылки - это аутентификация, канал передачи прав доступа не предоставляет. Важно, чтобы код или magic link генерировал и проверял российский сервис, а иностранный провайдер не получал доступ к учетной записи.

? А сами сервисы доставки: SMS-агрегаторы и рассыльщики?

Под ч.10 ст.8 они не подпадают: авторизация остается на стороне ресурса. Риски здесь по 152-ФЗ - поручение на обработку, локализация и уведомление о ТПД, если провайдер иностранный.

? Okta, PingID, Microsoft Entra ID - можно ли оставить?

Нет, если вход пользователей в РФ идет на их стороне (п.4 ч.10 ст.8). Свой Keycloak допустим с мерами защиты по ст.16 149-ФЗ, если более 50% голосов в компании у российской стороны. Иначе нужны номер, ЕСИА, ЕБС или SSO российского владельца.

Риск-ориентированный подход

С каких ресурсов начинать приведение авторизации в соответствие

Privacy Advocates

ТИП РЕСУРСА	Явно заметные вход виден любому со стороны	Неявно заметные о входе знает ограниченный круг
Внешние ресурсы для клиентов и посетителей	**Приоритет 1 — Критический риск** Нарушение видно из браузера без усилий, кнопка иностранного входа попадает в мониторинг РКН и в жалобы пользователей. Устраняем в первую очередь сайт с формой входа, мобильное приложение в сторах, интернет-магазин, личный кабинет клиента	**Приоритет 2 — Высокий риск** Обнаруживается по жалобе, при сканировании поддоменов или при проверке интеграции с партнером. Правим сразу после публичных сервисов партнерский портал по приглашению, админ-панель CMS на публичном домене, API и вебхуки, тестовые стенды
Внутренние ресурсы для сотрудников и подрядчиков	**Приоритет 3 — Средний риск** Изъятий для корпоративных сервисов нет. Выявляется по жалобе сотрудника или при проверке. Планируем на ближайший цикл релизов корпоративная почта и таск-трекер на Google Workspace, HR-портал, Jira и Confluence, вход в VPN	**Приоритет 4 — Базовый риск** Вероятность обнаружения низкая, но нарушение остается нарушением. Закрываем в плановом порядке при инвентаризации и обновлении систем системы закрытого контура, служебные админ-панели, тестовые среды, встроенное ПО

Матрица задает очередность, а не освобождает от требования: изъятий для внутренних и незаметных ресурсов в ч.10 ст.8 149-ФЗ нет, а ответственность по ст.13.55 КоАП действует с 07.07.2026

23.4

Антифрод-3

- Перспективы: Антифрод-3
- Антифрод-3: расширение круга лиц
- Антифрод-3: способы и смежные новеллы

Перспективы: Антифрод-3

Третий пакет мер против правонарушений с использованием ИКТ

Privacy Advocates

Законопроект о поправках в закон "О связи" и смежные акты, разработан Минцифры России во исполнение протокола совещания у Д.Ю. Григоренко от 27.04.2026, опубликован для общественного обсуждения 30.09.2026.

Апрель 2026

Поручение по итогам совещания у Д.Ю. Григоренко - основание для разработки проекта Минцифры.

Август 2026

После согласования в госорганах и Банке России редакция от 19.08.2026 вышла без нормы о хранении.

Сентябрь 2026

В опубликованной 30.09.2026 редакции трехлетнее хранение сведений о входах возвращено.

Март 2028

Планируемая дата вступления новых требований в силу - 1 марта 2028 года.

Антифрод-3: расширение круга лиц

Новая редакция ч.10 ст.8 149-ФЗ: кто обязан и что придется хранить

Privacy Advocates

НОВАЯ РЕДАКЦИЯ Ч.10

Круг обязанных лиц расширяется



СЕЙЧАС

ПРОЕКТ

Иностранные ресурсы теряют изъятие: вход только через иностранные SSO больше не вариант.

Иностранным владельцам - только вход по номеру телефона для пользователей в РФ (ч.10.1-1).

Норма о хранении возвращена

3 года хранения сведений о регистрации, авторизациях и прекращении регистрации пользователей (п.2 ч.10)

- Выдача органам ОРД и безопасности по правилам Правительства РФ
- При входе через ЕСИА сведения об авторизациях хранятся в ЕСИА (ч.10.1-2)
- Проект опубликован 30.09.2026, вступление в силу 01.03.2028

Часть 10.1 для российских владельцев и роль абонентского номера

Privacy Advocates

Новая ч.10.1

ДЛЯ РОССИЙСКИХ ВЛАДЕЛЬЦЕВ

- **Абонентский номер**
- **ЕСИА**
- **ЕБС**
- **Иная ИС**

- Условие о защите информации для "иной ИС" (ст.16 149-ФЗ) действует и сейчас
- Российское юрлицо - более 50% голосов у РФ, региона, муниципалитета или россиян без второго гражданства

Ч.10.1-1 закрывает вопрос: иностранцам - только номер, российским - любой из четырех, причем без оговорки о пользователях в РФ.

СМЕЖНЫЕ НОВЕЛЛЫ

ГИС "Антифрод"

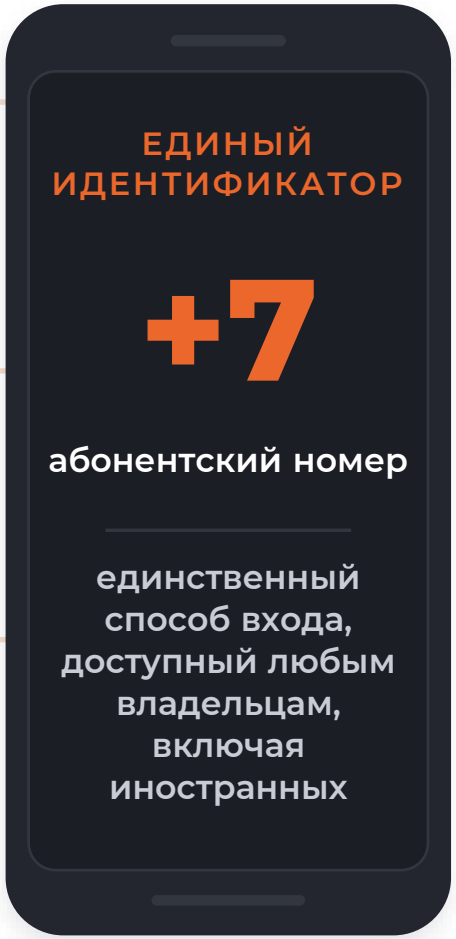
хранит данные для входа, используемые причастными к нарушениям (ч.5 ст.1 41-ФЗ)

Идентификация абонентов

усиливается, в том числе через ЕСИА и ЕБС при дистанционном договоре связи

Сим-карты

запрет перепродажи сим-карт с уже выделенным номером



КЛЮЧЕВЫЕ ВЫВОДЫ

- Российские ресурсы авторизуют пользователей в РФ одним из четырех способов; иностранные сервисы входа - Apple ID, Google Sign-In - под запретом.
- Требование привязано к местонахождению пользователя, а не к гражданству. За нарушение действует ст.13.55 КоАП, а ст.274.5 УК касается передачи данных авторизации.
- Проект Антифрод-3 (вступление 01.03.2028) распространит требование на иностранные ресурсы и вернет трехлетнее хранение сведений о регистрации и входах с выдачей силовым органам.

24

Искусственный интеллект и ПД

Практический гайд по комплаенсу защиты данных при использовании ИИ

24.1 Устройство ИИ и зоны риска

24.2 Тайны, персонал и ответственность

24.3 ПД в ИИ-сервисах

24.4 Управление ИИ в компании

24.5 Обучение моделей и решения ИИ

Раздел на сайте
privacy-advocates.ru/pd/aig

РАЗДЕЛ 24. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПД

24.1

Устройство ИИ и зоны риска

- Матрица того, где не стоит применять ИИ
- Семь уровней ИИ
- Как устроена ИИ-система
- Анатомия ИИ-системы: где живут риски

Матрица того, где не стоит применять ИИ

Если ИИ что-то может, это еще не значит, что он должен это делать

Privacy Advocates

Цена ошибки

высокая

низкая

ИИ готовит, решает человек

Финансовая отчетность
Юридические документы
Медицинские заключения

Решает только человек

Наем и увольнение
Этический выбор
Кризисные ситуации

ИИ справится сам

Расшифровка записей
Краткие изложения
Форматирование

ИИ пишет, человек правит

Посты и рассылки
Деловая переписка
Мозговой штурм

низкая — **Необходимость вовлечения человека** — высокая

Семь уровней ИИ

Путь от правил и логики к общему интеллекту

Privacy Advocates

Каждый уровень опирается на предыдущий.
Чем выше, тем больше ИИ действует сам.

7 **Общий ИИ (AGI)**
универсальный интеллект, пока не достигнут

ТЕКУЩИЙ РУБЕЖ

6 **Агентный ИИ**
планирует, использует инструменты и действует

МЫ ЗДЕСЬ

5 **Генеративный ИИ**
создает тексты, изображения, аудио и код

ChatGPT · Claude · Gemini · Midjourney

4 **Глубокое обучение**
многослойные нейросети для зрения, речи и языка

3 **Нейронные сети**
взаимосвязанные представления, выученные из данных

2 **Машинное обучение**
находит закономерности в данных

1 **Классический ИИ**
правила, логика, поиск

Как устроена ИИ-система

Та же архитектура, что у компьютера, только на новой основе

Privacy Advocates

Компьютер	ИИ-система
Процессор	Языковая модель (LLM) и ее веса
Оперативная память	Контекстное окно
Жесткий диск	Векторная база и долговременная память
Драйверы устройств	Интеграции с инструментами
Операционная система	Обвязка системы (harness)
Приложение	Агент (эмерджентное поведение)

Анатомия ИИ-системы: где живут риски

Шесть слоев, и у каждого своя зона комплаенса

Privacy Advocates

Фильтры и журналы

Единый шлюз запросов к моделям, DLP, защита от инъекций. Журналы вызовов тоже хранят ПД

Что уходит в запрос

Инструкция, файлы, фрагменты базы знаний. Очистка от ПД и сведений под тайной до отправки

Где исполняется и чему учится

Локализация и ТПД по месту первой записи, дообучение поставщика, с 01.03.2027 ЦОД в России для суверенных моделей



1

Полномочия и результат

Права агента не шире прав пользователя. Отправка вовне и необратимые действия только после подтверждения человеком

2

3

Новые получатели данных

Почта, CRM, поиск, другой агент. Каждое подключение проверяется как привлечение подрядчика

4

5

Память и права субъекта

Сроки, доступы, уточнение и удаление по запросу субъекта, в том числе в памяти агента

6

Оранжевые слои обрабатывают запрос, темные хранят знания и модель. Карту потоков данных собирают по всем шести слоям

Что изменилось за год

Нормы и судебные акты 2025-2027, которые меняют правила работы с ИИ

Privacy Advocates

01.09.2025
Обезличивание по новым правилам
Требования и методы из приказа РКН № 140 обязательны для всех операторов

01.03.2026
ИИ-блок приказа ФСТЭК № 117
В госсистемах нельзя передавать разработчику модели информацию ограниченного доступа

14.05.2026
Штраф за выдуманные ссылки
Судебный штраф 50 000 ₽ за несуществующую практику в жалобе, ИИ не оправдание

26.05.2026
Нейросеть как канал разглашения
Первая инстанция учла выгрузку тайны в нейросеть при увольнении, отдельно ее не квалифицируя

01.09.2026
Вступил в силу 243-ФЗ
Закон о поддержке технологий ИИ, основной блок требований к большим моделям с 01.03.2027

07.09.2026
Концепция цифровой грамотности
Обучение персонала работе с ИИ предложено встроить в управление рисками

сейчас

01.03.2027
Суверенные модели и пометка ИИ
ЦОД в России, право пометить ИИ-контент, изъятие для обучения, проект нового ИИ-блока ФСТЭК

01.09.2032
Конец переходного периода
Для систем, работающих на 01.03.2027, при обработке данных в России

нормы
суды
ориентиры

24.2

Тайны, персонал и ответственность

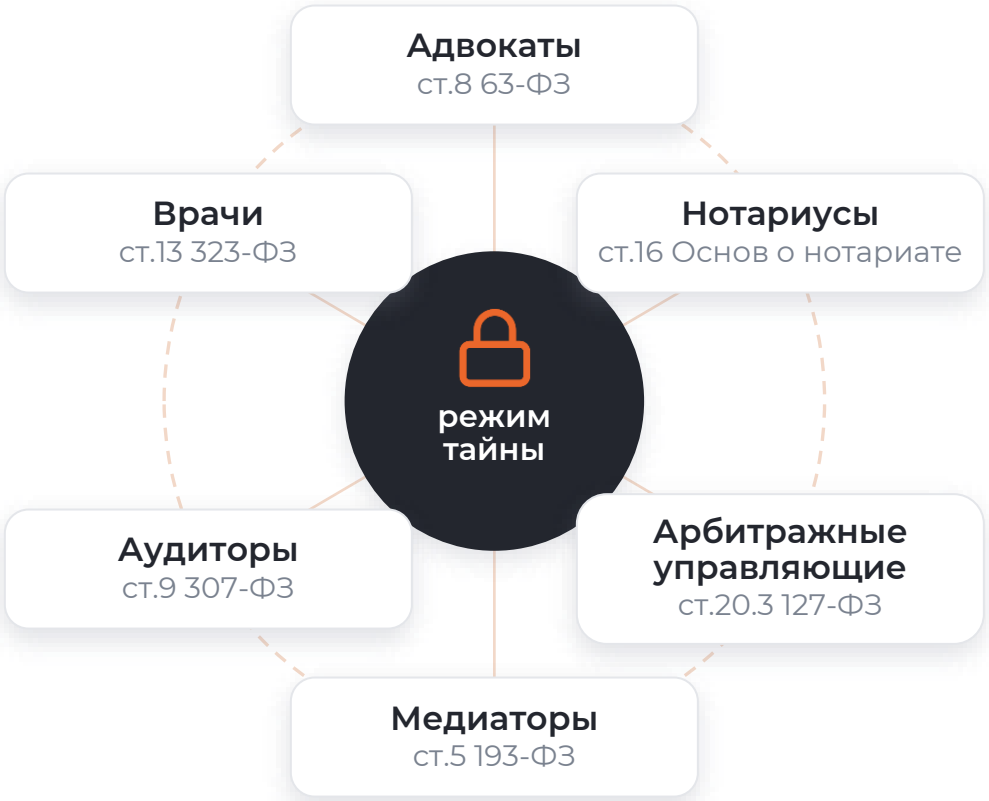
- Профессиональная тайна: второй замок
- Персонал и нейросеть
- Ответственность за ошибки ИИ
- ИИ-агенты: контур шире окна диалога

Профессиональная тайна: второй замок

Очистка от ПД не снимает режима тайны, а передача сервису уже разглашение

Privacy Advocates

КОГО КАСАЕТСЯ



А также банковская, налоговая, страховая тайна и коммерческая тайна самого клиента

ДВА ФИЛЬТРА ПЕРЕД ЗАГРУЗКОЙ



1 Фильтр ПД

Убирает ФИО, контакты, номера договоров и иные идентификаторы

2 Фильтр тайны

Цифры, метрики, конструкция сделки и сведения о компаниях остаются тайной и без имен

Передача сервису уже разглашение

Поставщик сервиса третье лицо, наступления утечки для нарушения не нужно

Согласие субъекта ПД не заменяет согласия клиента

Раскрыть тайну позволяет только волеизъявление клиента, и его форма бывает строже

Право на ИИ закрепляется в договоре

Заранее, в соглашении с клиентом. Материалы все равно проходят оба фильтра

Персонал и нейросеть

Запрещать стоит не инструмент, а вынос сведений

Privacy Advocates

ТРИ ЗОНЫ ПО МЕСТУ ИСПОЛНЕНИЯ ЗАПРОСА

Своя модель в контуре

Данные не покидают периметр, систему можно настроить под задачи

Внешняя модель по API

Допустимо после локального акта, договора и технического фильтра

Публичный сервис, личный аккаунт

Оправданий нет, эта зона закрывается первой

БАБУШКИНСКИЙ РАЙОННЫЙ СУД Г. МОСКВЫ

РЕШЕНИЕ ОТ 26.05.2026, ДЕЛО № 02-1545/2026

Загрузка отчетов в DeepSeek признана разглашением коммерческой тайны

Отчеты о сделках и финансах ушли в DeepSeek, тендерные документы на личную почту. Увольнение признано законным, а дошли ли сведения до третьих лиц, значения не имеет

Доказательства режима в деле: перечень сведений, обязательство под подпись, контроль рабочих мест и акт расследования

ТРОЙКА МЕР ВМЕСТО ЗАПРЕТА

Режим тайны

Перечень сведений, порядок обращения, обязательство работника под подпись

Удобная внутренняя площадка

Без нее работники уходят в личные аккаунты и обходные каналы

Контроль исходящего трафика

DLP и единый шлюз для обращений к внешним моделям

Личные аккаунты в рабочих задачах запрещаются прямо, допустимые сервисы перечисляются в локальном акте

Ответственность за ошибки ИИ

За точность результата отвечает тот, кто его применил

Privacy Advocates

ОПРЕДЕЛЕНИЕ АС ЗСО ОТ 14.05.2026

ДЕЛО № А27-7831/2025

50 000 ₽

судебный штраф за несуществующую и чужую практику в кассационной жалобе

- Половина максимума и вровень с суммой основного долга по спору
- Штраф наложен на организацию, а не на ее представителя
- Подготовка с помощью ИИ не оправдание, за сгенерированный текст отвечает участник дела, ч.2 ст.9 АПК
- Просьба нового представителя не учитывать ссылки от штрафа не спасла
- В жалобе были и чужие акты. Реальный номер с посторонним предметом проходит формальную сверку

ТРИ ЛИНИИ ЗАЩИТЫ

Договор с поставщиком ответственности не перераспределяет, спрос будет с компании, которая применила ИИ

01 **Процедура**
Финальные действия без проверки человеком запрещены в регламентах, скриптах и инструкциях. Проверка выборочная, с критериями эскалации

02 **Договор**
Предупреждение клиента о применении ИИ, согласие на передачу данных, лимиты ответственности

03 **Доказательства**
Следы проверки и уведомления клиента. Кто проверил, когда и что исправил

Перед подачей наружу каждая ссылка проверяется по трем признакам: **акт существует, его предмет совпадает с тезисом, цитата в нем действительно есть**

ИИ-агенты: контур шире окна диалога

Чем больше полномочий у агента, тем шире зона ответственности компании

Privacy Advocates

ЧТО ВХОДИТ В КОНТУР ОБРАБОТКИ



Каждый элемент хранит ПД со своими сроками и доступами. Темным отмечено то, что чаще всего забывают

ТРИ СЦЕНАРИЯ ОТКАЗА

Избыточный сбор
объем данных выходит за пределы цели

Передача вовне
сведения уходят третьему лицу без основания

Утрата данных
стерты записи, которые полагалось хранить

ЧЕТЫРЕ БАРЬЕРА

- **Закрытый перечень действий агента**
- **Права агента не шире прав пользователя**
- **Подтверждение человеком любой отправки вовне**
- **Запрет необратимых операций**

Отдельный риск инъекции. Скрытая команда в файле или на странице исполняется наравне с указанием пользователя

24.3

ПД в ИИ-сервисах

- Персональные данные: маскирование не анонимность
- Поставщик ИИ: обработчик или оператор
- Зарубежные сервисы: локализация
- Трансграничная передача

Персональные данные: маскирование не анонимность

Самый безопасный сценарий: не загружать ПД в сервис вообще

Privacy Advocates

ШКАЛА ИДЕНТИФИЦИРУЕМОСТИ

действует 152-ФЗ | вне режима ПД

Исходные ПД	Маскирование и псевдонимы	Обезличивание по приказу РКН № 140	Агрегаты без выделения лица
ФИО, телефоны, номера договоров	Имена заменены, связи и детали на месте	По позиции РКН все еще ПД	Группы, где нельзя выделить человека

ЧТО ВАЖНО ЗНАТЬ

- С 01.09.2025 требования и методы обезличивания из приказа РКН № 140 обязательны для всех операторов
- Обезличивание само является обработкой и требует основания и цели
- Модель может вывести здоровье или убеждения из обычных данных, и такой вывод уже спецкатегория по ст.10 152-ФЗ

ЧТО ДЕЛАТЬ

- Очищать данные до того, как они покидают контур компании
- Выяснить, что и в каком виде персонал реально загружает в ИИ
- Так же обращаться с любой чувствительной информацией, особенно в иностранных сервисах

Обезличенные данные все равно персональные. Маскирование от требований 152-ФЗ не освобождает

Поставщик ИИ: обработчик или оператор

Квалификация зависит от того, что поставщик делает с вашими данными

Privacy Advocates

Что поставщик делает с полученными данными?

Только выполняет ваш запрос

Поручение обработки

Договор с перечнем действий, целями, конфиденциальностью и требованиями к защите. Перед субъектом отвечаете вы

Учится на них или использует в своих целях

Самостоятельный оператор

Нужно свое основание передачи, обычно согласие. Дообучение по умолчанию разрушает конструкцию поручения

ЧЕТЫРЕ СКРЫТЫХ КАНАЛА

Дообучение

Включено по умолчанию, на части тарифов не отключается

Кнопка оценки

Возвращает данные поставщику даже при выключенном обучении

Лицензия на диалог

Запросы и файлы нередко уходят под безотзывную лицензию

Экспортный контроль

Блокировка аккаунта вместе с материалами, копии держите вне сервиса

Данные пришли от контрагента? Сначала проверьте в договоре с ним, разрешены ли субобработчики. А корпоративная подписка сама по себе передача ПД работников

Зарубежные сервисы: локализация

Где первичное сохранение данных нарушает требование о локализации

Privacy Advocates

Скрытая зарубежная модель

Внутри российского продукта незаметно для пользователя может работать иностранная модель - отечественная вывеска не гарантирует, что данные остаются в РФ.

Первичное сохранение за рубежом

Расшифровка встреч или чат-бот на иностранной платформе: первая запись происходит на серверах за границей, и требование локализации не выполняется.

Сначала в РФ, потом за рубеж

Когда ПД сначала записываются в базу в РФ и лишь затем передаются зарубежному получателю по правилам ТПД, локализация соблюдена.

Суверенная модель с 01.03.2027

Ответы и хранение в ЦОД российского юрлица. Для локализации собственник ЦОД значения не имеет, для 243-ФЗ имеет

ШТРАФЫ ЗА ЛОКАЛИЗАЦИЮ

6 млн ₽

максимум за первое нарушение

18 млн ₽

максимум за повторное нарушение

Разберите маршруты данных в продукте с оглядкой на то, как им реально пользуются сотрудники.

чч.8, 9 ст.13.11 КоАП, для юрлиц

Трансграничная передача

Использование зарубежного ИИ - это трансграничная передача данных

Privacy Advocates

Порядок до начала передачи

1. Подать в Роскомнадзор уведомление о трансграничной передаче.
2. Запросить у зарубежного получателя сведения о применяемой защите данных.
3. Рассчитывать на документы провайдера не стоит - оценку придется собирать по открытым источникам.

По позиции РКН (14.08.2026) ТПД возникает между операторами. Человек, сам вводящий свои данные в зарубежную нейросеть, ее не совершает

ПЕРЕЧЕНЬ СТРАН: ПРИКАЗ РКН № 128, С 30.10.2026 № 253

Страна в перечне

Передавать можно сразу после уведомления

КИТАЙ | ЕС

Страны нет в перечне

Старт передачи - через 10 рабочих дней, и за РКН остается право запрета.

США - УСЛОЖНЕННЫЙ ПОРЯДОК

Корпоративная подписка - провайдер получает ПД сотрудников, на что обычно требуется их письменное согласие в строгой форме.

Закон об ИИ 243-ФЗ: что важно пользователю

Закон регулирует большие фундаментальные модели и режим ПД не отменяет

Privacy Advocates

ПОПАДАЕТ ЛИ МОДЕЛЬ ПОД ЗАКОН



Все три признака сразу дают большую фундаментальную модель (БФМ). Скоринг, антифрод и компьютерное зрение живут по общим правилам 152-ФЗ

С 01.03.2027

ЦОД российских юрлиц

Суверенные и национальные модели готовят ответы и хранят данные в России. Это не то же самое, что локализация

Обязательные случаи

Правительство вправе определить, где допустимы только такие модели, в финсекторе по согласованию с Банком России

Изъятие для обучения

Снимает вопрос авторских прав, но не ПД. Для сведений о людях нужно свое основание

Переход до 01.09.2032

Для систем, работающих на 01.03.2027, если данные обрабатываются и хранятся в России

Что сделать сейчас: составить перечень моделей и их статус, зафиксировать дату ввода и место обработки, предусмотреть в договоре с поставщиком замену модели

24.4

Управление ИИ в компании

- Управление ИИ в компании: семь шагов
- Чек-лист перед запуском ИИ

Управление ИИ в компании: семь шагов

Каждый шаг оставляет документ, иначе процесс не доказать

Privacy Advocates

Владелец

У каждого ИИ-сервиса есть ответственное лицо



Реестр ИИ-решений

Сценарий, модель, поставщик, данные, инструменты, уровень автономности

Правила использования

Что можно загружать и делать, где обязателен человек

Оценка рисков до запуска

Запуск, дополнительные меры, ограничение сценария или отказ

Точка контроля

Без пройденных проверок сервис не выпускается

Управление изменениями

Смена модели, поставщика, инструкции или базы знаний возвращает к оценке

Мониторинг и инциденты

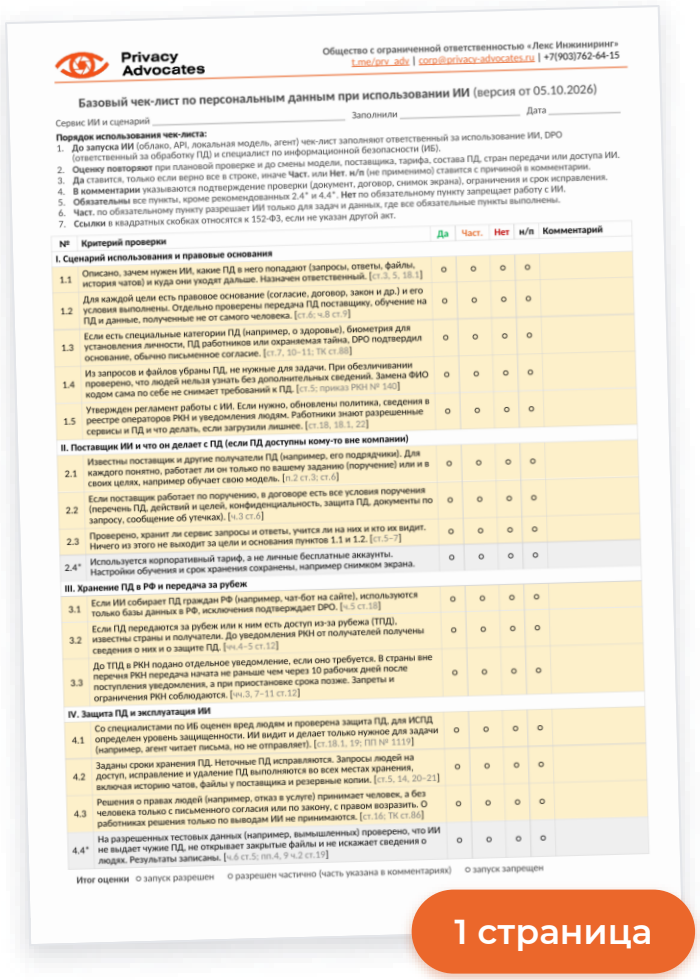
Метрики качества, жалобы, ошибки и корректирующие меры

См: ст.18.1 152-ФЗ и ГОСТ Р ИСО/МЭК 42001-2024 о системе менеджмента ИИ

Чек-лист перед запуском ИИ

Одна страница, чтобы до запуска понять, можно ли доверить ИИ персональные данные

Privacy Advocates



Privacy Advocates

Общество с ограниченной ответственностью «Лекс Инжиниринг»
t.me/priv_adv | corp@privacy-advocates.ru | +7(903)762-64-15

Базовый чек-лист по персональным данным при использовании ИИ (версия от 05.10.2026)

Сервис ИИ и сценарий _____ Заполнили _____ Дата _____

Порядок использования чек-листа:

1. **До запуска ИИ** (облако, API, локальная модель, агент) чек-лист заполняют ответственный за использование ИИ, DPO (ответственный за обработку ПД) и специалист по информационной безопасности (ИБ).
2. **Оценку повторяют** при плановой проверке и до смены модели, поставщика, тарифа, состава ПД, стран передачи или доступа ИИ.
3. **Да** ставится, только если верно все в строке, иначе **Част.** или **Нет**. **н/п** (не применимо) ставится с причиной в комментарии.
4. **В комментарии** указываются подтверждение проверки (документ, договор, снимок экрана), ограничения и срок исправления.
5. Обязательны все пункты, кроме рекомендованных 2.4* и 4.4*. **Нет** по обязательному пункту запрещает работу с ИИ.
6. **Част.** по обязательному пункту разрешает ИИ только для задач и данных, где все обязательные пункты выполнены.
7. Ссылки в квадратных скобках относятся к 152-ФЗ, если не указан другой акт.

№	Критерий проверки	Да	Част.	Нет	н/п	Комментарий
I. Сценарий использования и правовые основания						
1.1	Описано, зачем нужен ИИ, какие ПД в него попадают (запросы, ответы, файлы, история чатов) и куда они уходят дальше. Назначен ответственный. [ст. 3, 5, 18.1]	○	○	○	○	
1.2	Для каждой цели есть правовое основание (согласие, договор, закон и др.) и его условия выполнены. Отдельно проверены передача ПД поставщику, обучение на ПД и данные, полученные не от самого человека. [ст.6; ч.8 ст.9]	○	○	○	○	
1.3	Если есть специальные категории ПД (например, о здоровье), биометрия для установления личности, ПД работников или охраняемая тайна, DPO подтвердил основание, обычно письменное согласие. [ст.7, 10–11; ТК ст.88]	○	○	○	○	
1.4	Из запросов и файлов убраны ПД, не нужные для задачи. При обезличивании проверено, что людей нельзя узнать без дополнительных сведений. Замена ФИО кодом сама по себе не снимает требований к ПД. [ст.5; приказ РКН № 140]	○	○	○	○	
1.5	Утвержден регламент работы с ИИ. Если нужно, обновлены политика, сведения в реестре операторов РКН и уведомления людям. Работники знают разрешенные сервисы и ПД и что делать, если загрузили лишнее. [ст.18, 18.1, 22]	○	○	○	○	
II. Поставщик ИИ и что он делает с ПД (если ПД доступны кому-то вне компании)						
2.1	Известны поставщик и другие получатели ПД (например, его подрядчики). Для каждого понятно, работает ли он только по вашему заданию (поручение) или и в своих целях, например обучает свою модель. [ч.2 ст.3; ст.6]	○	○	○	○	
2.2	Если поставщик работает по поручению, в договоре есть все условия поручения (перечень ПД, действий и целей, конфиденциальность, защита ПД, документы по запросу, сообщение об утечках). [ч.3 ст.6]	○	○	○	○	
2.3	Проверено, хранит ли сервис запросы и ответы, учится ли на них и кто их видит. Ничего из этого не выходит за цели и основания пунктов 1.1 и 1.2. [ст.5–7]	○	○	○	○	
2.4*	Используется корпоративный тариф, а не личные бесплатные аккаунты. Настройки обучения и срок хранения сохранены, например снимком экрана.	○	○	○	○	
III. Хранение ПД в РФ и передача за рубеж						
3.1	Если ИИ собирает ПД граждан РФ (например, чат-бот на сайте), используются только базы данных в РФ, исключения подтверждает DPO. [ч.5 ст.18]	○	○	○	○	
3.2	Если ПД передаются за рубеж или к ним есть доступ из-за рубежа (ТПД), известны страны и получатели. До уведомления РКН от получателей получены сведения о них и о защите ПД. [ч.4–5 ст.12]	○	○	○	○	
3.3	До ТПД в РКН подано отдельное уведомление, если оно требуется. В страны вне перечня РКН передача начата не раньше чем через 10 рабочих дней после поступления уведомления, а при приостановке срока позже. Запреты и ограничения РКН соблюдаются. [ч.3, 7–11 ст.12]	○	○	○	○	
IV. Защита ПД и эксплуатация ИИ						
4.1	Со специалистами по ИБ оценен вред людям и проверена защита ПД, для ИСПД определен уровень защищенности. ИИ видит и делает только нужное для задачи (например, агент читает письма, но не отправляет). [ст.18.1, 19; ПП № 1119]	○	○	○	○	
4.2	Заданы сроки хранения ПД. Неточные ПД исправляются. Запросы людей на доступ, исправление и удаление ПД выполняются во всех местах хранения, включая историю чатов, файлы у поставщика и резервные копии. [ст.5, 14, 20–21]	○	○	○	○	
4.3	Решения о правах людей (например, отказ в услуге) принимает человек, а без человека только с письменного согласия или по закону, с правом возразить. О работниках решения только по выводам ИИ не принимаются. [ст.16; ТК ст.86]	○	○	○	○	
4.4*	На разрешенных тестовых данных (например, вымышленных) проверено, что ИИ не выдает чужие ПД, не открывает закрытые файлы и не искажает сведения о людях. Результаты записаны. [ч.6 ст.5; пп.4, 9 ч.2 ст.19]	○	○	○	○	

Итог оценки ○ запуск разрешен ○ разрешен частично (часть указана в комментариях) ○ запуск запрещен

1 страница

16 ПУНКТОВ В ЧЕТЫРЕХ БЛОКАХ

I. Цели и основания
Зачем нужен ИИ, какие данные в него попадают и на каком основании

II. Поставщик ИИ
Кто видит данные, хранит ли их и учится ли на них

III. Хранение и передача за рубеж
Где лежат данные и есть ли к ним доступ из других стран

IV. Защита и контроль
Доступы ИИ, сроки хранения, решения о людях и тесты

ИТОГ ПО ОБЯЗАТЕЛЬНЫМ ПУНКТАМ

Да — запуск разрешен

Част. — ограниченный запуск

Нет — запуск остановлен

ОТКРЫТЬ ЧЕК-ЛИСТ

Скачать с Яндекс Диска

Актуальная версия для скачивания и заполнения

24.5

Обучение моделей и решения ИИ

- Обучение модели на ПД безопаснее считать отдельной целью
- Массив для обучения надежнее обезличить до старта
- Скоринговая оценка сама становится ПД о человеке
- Смещение модели ищут по результату, а не по признакам

Обучение модели на ПД безопаснее считать отдельной целью

Признаки самостоятельной цели, спор о совместимости и узкие коридоры оснований ч.1 ст.6 152-ФЗ

Privacy Advocates

ПРИЗНАКИ ОТДЕЛЬНОЙ ЦЕЛИ, ЭКСПЕРТНЫЙ ПОДХОД

1. результат обучения применяют за пределами процесса, где собраны данные
2. модель передают или предоставляют третьим лицам
3. обучение идет в интересах разработчика, а не субъекта или заказчика

ЦЕЛИ НЕ ВОЗНИКАЕТ

обучение внутри того же процесса и цели, как антифрод платежного сервиса. Спорно, совместимо ли оно с целью сбора, если модель не выходит за сервис

ОСНОВАНИЕ	КОРИДОР ДЛЯ ОБУЧЕНИЯ
Согласие, п.1	держит плохо: массив не собрать, вклад отозвавшего из модели не извлечь, будущие задачи не конкретны
Исследования, п.9	с обязательным обезличиванием и без решений о лицах, Роскомнадзор устно (01.03.2023) включал оценку поведения в маркетинге, практики нет
Обезличенные ПД, п.9.1	только госуправление, экспериментальные режимы и государственные составы данных
Законный интерес, п.7	собственный процесс оператора без специальных категорий и с тестом соразмерности
Договор, п.5	если модель и есть содержание заказанной услуги

Документы: цель обучения объявляют отдельно в политике, уведомлении, основании и оценке вреда, а формула о развитии технологий требованию конкретности не отвечает

Массив для обучения надежнее обезличить до старта

Три ветви работы с данными, разметка, сбор из открытых источников и выпуск модели с открытыми весами

Privacy Advocates

1

Ветвь А. Обезличить

с проверкой на реидентификацию, результат Роскомнадзор устно считает ПД (28.01.2022, 27.08.2025, 14.08.2026)

2

Ветвь Б. Найти основание

на исходных данных: исследования, законный интерес или договор

3

Ветвь В. Собрать заново

под объявленную цель обучения со своим сроком хранения выборки

СИТУАЦИЯ	ЧТО УЧЕСТЬ
Обезличивание	само обработка с основанием и целью (Роскомнадзор 25.11.2022, 24.08.2023). Согласие вне пп.9, 9.1 спорно: Минцифры (21.10.2022) за, Роскомнадзор устно (28.01.2022) таких случаев не видит
Разметка вовне	поручение по ч.3 ст.6, зарубежная площадка добавляет локализацию и ТПД
Открытые источники	до сбора два заключения, об основании обработки ПД и о правах изготовителя базы (ст.1334 ГК)
Открытые веса	по экспертному подходу корпус из весов не восстановить, но запомненное доступнее, и тесты на запоминание идут до релиза

Эксперимент: в экспериментальных режимах по 123-ФЗ и 258-ФЗ требования приказа Роскомнадзора № 140 к обезличиванию не применяются, а п.9.1 ч.1 ст.6 доступен только участникам в пределах программы

Скоринговая оценка сама становится ПД о человеке

Кредитный, страховой, кадровый и антифрод-скоринг: основания признаков, ст.16 152-ФЗ и пробел практики

Privacy Advocates

СКОРИНГ	ЧТО ЗАТРАГИВАЕТ	МАРШРУТ
Кредитный	отчет по 218-ФЗ требует согласия, но покупки, запросы и устройство в модели выводят в общий режим 152-ФЗ	основание по каждому источнику признаков и отдельно по ч.2 ст.16
Страховой	коэффициент задает цену договора и затрагивает права, разница цен по месту жительства или полу, по экспертному подходу, риск дискриминации	проверка основания и признаков, КТ в ОСАГО прямо задан Указанием № 6007-У
Кадровый	отбраковка и ранжирование резюме, ТК соискателей не регулирует (Роскомнадзор устно 31.01.2024, 14.08.2026), п.6 ст.86 лишь по аналогии	итог за представителем работодателя и доступ ко всем резюме
Антифрод	блокировка, приостановка и допроверка затрагивают права, а согласие невозможно	закон с мерами защиты или решение за человеком

ОТКРЫТАЯ ПЛОЩАДКА

признаки из соцсетей и объявлений требуют своего основания и строки в уведомлении (А40-5250/2017, решения 2017-2018 годов). Опубликованное по закону идет по п.11 ч.1 ст.6, развилка спорна

ПРОБЕЛ ПРАКТИКИ

споры по кредитным историям идут об изъятии записи о просрочке (33-44119/2021, 88-8554/2022) и о согласии на отчет (А56-47954/2021), а об исключительно автоматизированном решении суды не спрашивают

Смещение модели ищут по результату, а не по признакам

Прокси-признаки, исторические выборки и проверка в шесть шагов до запуска и при каждом переобучении

Privacy Advocates

СОСТАВА НЕТ

Риск идет смежными маршрутами

общий запрет дискриминации ст.3 и 64 ТК, запрет дискриминационных вакансий, ст.16 ЗоЗПП и равенство по ст.19 Конституции. Достаточность этих маршрутов спорна

МЕХАНИКА СМЕЩЕНИЯ, ЭКСПЕРТНЫЙ ПОДХОД

- почтовый индекс заменяет этническую принадлежность, а профессия и тип образования заменяют пол
- выборка повторяет прошлые решения, а малочисленные группы модель принижает

РЕКОМЕНДУЕМАЯ ПРОВЕРКА ДО ЗАПУСКА И ПРИ ПЕРЕОБУЧЕНИИ

1. **Убрать прямые признаки**
   защищаемые характеристики исключают из модели
2. **Найти прокси**
   восстанавливается ли признак по остальным атрибутам
3. **Проверить выборку**
   смещение состава и малая представленность групп
4. **Сравнить группы**
   доли положительных и отрицательных выводов
5. **Отсечь спецкатегории**
   вывод о здоровье или убеждениях требует основания
6. **Записать протокол**
   дата, состав и результаты как доказательство

Ориентир: Стратегия развития ИИ (Указ № 490 от 10.10.2019) называет защиту ПД при обучении моделей среди вызовов, обязанностей не создает, но служит ориентиром добросовестности

Реальное участие человека в решении видно по журналу отклонений

Содержательное участие, причины вырождения контроля и обязанности оператора по чч.3 и 4 ст.16 152-ФЗ

Privacy Advocates

ПРИЗНАКИ УЧАСТИЯ, ЭКСПЕРТНЫЙ ПОДХОД

1. решающий видит первичные данные и отбракованный системой массив
2. может решить вопреки подсказке без последствий для себя
3. доля расхождений с подсказкой не нулевая и пишется в журнал

ПОЧЕМУ КОНТУР ВЫРОЖДАЕТСЯ

по экспертному подходу, мешают доверие к системе, нехватка времени на проверку и потеря навыка. Помогают выборка, четыре глаза и эскалация

ОБЯЗАННОСТЬ	СОДЕРЖАНИЕ
Разъяснить порядок, ч.3	порядок решения и возможные юридические последствия без раскрытия алгоритма, категории данных и источники по экспертному прочтению, глубина спорна
Принять возражение, ч.3	процедуру оператор устанавливает сам и разъясняет порядок защиты прав
Ответить за 30 дней, ч.4	со дня получения, а не в рабочих днях ст.14 и ст.20
Итог возражения	отмена, пересмотр человеком или пересчет, закон молчит, вопрос спорен

Практика: у ст.16 почти нет собственной практики: Оренбургский облсуд в деле 33-7486/2015 проверил только подпись под общими условиями. Механику решения раскрывают надзорная проверка и смежный спор

КЛЮЧЕВЫЕ ВЫВОДЫ

- Обезличивание не снимает ограничений: замаскированные данные остаются персональными и живут по правилам 152-ФЗ.
- Профессиональная и коммерческая тайна требуют второго фильтра: очистка от ПД режима тайны не снимает.
- Спрос за результат ИИ с пользователя, а не с провайдера, поэтому финальные шаги без проверки человеком под запретом.
- Иностранный сервис ставит вопросы локализации и трансграницы, с 01.03.2027 добавится 243-ФЗ. Защиту готовят заранее.

25

Дипфейки

Правовой статус дипфейков в РФ и мире

25.1 Угроза и синтетические личности

25.2 Регулирование дипфейков

Раздел на сайте
privacy-advocates.ru/pd/dip

25.1

Угроза и синтетические личности

- Дипфейк-мошенничество растет, а глаз подделку уже не ловит
- Синтетический двойник отделяет облик и голос от человека

Дипфейк-мошенничество растет, а глаз подделку уже не ловит

Масштаб угрозы: рост атак, уязвимость государственных систем и смена парадигмы распознавания

Privacy Advocates

в разы

рост мошенничества с дипфейками

по оценкам рынка, в 2025 году атаки с синтезированными лицом и голосом кратно выросли

десятки млн $

обман госсистем в Китае

по сообщениям СМИ, атака на биометрическую проверку через перепрошитые смартфоны, подменявшие изображение для камеры

СМЕЩЕНИЕ ПАРАДИГМЫ

Визуальный контроль мертв

подделку теперь распознает только машина: ИИ против ИИ

- регуляторы признают, что качество дипфейков уже выше возможностей человеческого восприятия
- предъявление записи перестает надежно подтверждать присутствие человека

Для оператора: оператор, применяющий распознавание лица или голоса, закладывает синтезированное предъявление в модель угроз отдельной угрозой и проверяет устойчивость к нему при оценке эффективности мер

Синтетический двойник отделяет облик и голос от человека

Анатомия синтетической личности: исходная биометрия, цена создания и проблема атрибутивности

Privacy Advocates

1

Физический носитель

реальный человек с узнаваемыми обликом и голосом

2

Биометрия лица и голос

исходные образцы берут из открытых фото, видео и записей речи

3

Отделение сущностей

модель отделяет облик и голос от носителя и учится их воспроизводить

4

Синтетический двойник

цифровая копия, которую выдают за человека. Цена создания $5-38

ПРОБЛЕМА АТРИБУТИВНОСТИ

Связь двойника с человеком трудно доказать

чем точнее копия, тем сложнее подтвердить, кто изображен и кто создал материал

?

Двойник - это ПД?

да, если узнаваемы облик или голос: определяемость лица не зависит от того, происходило ли событие на записи

?

Создание копии - обработка биометрии?

нет, цель не установить личность, а выдать изображение за человека, поэтому письменное согласие по ст.11 не требуется, но режим ПД и охрана изображения действуют

25.2

Регулирование дипфейков

- Тотальная криминализация дипфейков рождает правовые коллизии
- Обязательную маркировку ИИ-видео заменила добровольная пометка
- Штрафы за немаркированный ИИ-контент остались проектом
- Мир регулирует дипфейки от запретов до фетв и гайдлайнов

Тотальная криминализация дипфейков рождает правовые коллизии

Инициативы наказывать за сам факт обработки и опора на уже действующие составы

Privacy Advocates

⚠ Новый состав

Наказание за сам факт обработки

- инициатива в Госдуме: наказание за сам факт обработки с правкой ст.272.1 УК
- загромождение статьи и дублирование норм
- признак "автоматизированная обработка" допускает расширительное толкование и задевает технологии ИИ и ML
- процессуальная эквилибристика: каждое дело требует описания конкретного технического кейса
- совет по кодификации не поддержал инициативу об изображении и голосе: термины не имеют четкого содержания

vs

⚖ Общие нормы

Усиление наказания по любому составу

- 14.07.2026 внесен проект о дипфейке как отягчающем обстоятельстве по ст.63 УК
- вопрос доказывания синтетического происхождения материала остается открытым
- изготовление ИИ-ботом изображения обнаженной натуры с лицом знакомой квалифицировано по п."б" ч.3 ст.242 УК, приговор устоял в апелляции (22-7749, 21.11.2025)
- сама технология синтеза не преступна

Сейчас: специального состава нет, и риск закрывают общие нормы: о ПД, об охране изображения, о клевете, мошенничестве и порнографии

675

Обязательную маркировку ИИ-видео заменила добровольная пометка

Судьба пакета о двойной маркировке и что ввел закон о развитии технологий ИИ 243-ФЗ

Privacy Advocates

14.11.2025

ВНЕСЕН ПАКЕТ

Двойная маркировка

видимая надпись на весь показ и неудаляемая машиночитаемая метка в метаданных: применение ИИ, дата, владелец ресурса

04.2026

КОМИТЕТ ДУМЫ

Рекомендовал отклонить

неясны обязанное лицо и стадия маркировки, сплошная проверка контента неисполнима

10.06.2026

ГОСДУМА

Пакет отклонен

вместе с ним отпал и состав КоАП о штрафах за отсутствие маркировки

01.09.2026

243-ФЗ

Закон об ИИ в силе

регулирует большие фундаментальные модели, обязанности маркировать не вводит

01.03.2027

СТ.9 243-ФЗ

Пометка добровольна

площадки с аудиторией свыше 500 тыс. в сутки лишь дают пользователю возможность ее разместить

ДЛЯ ОПЕРАТОРА ПД

Пометка ничего не доказывает

немаркированный материал не доказывает подлинности, а пометка не меняет оценки чужого облика или голоса по правилам о ПД и об изображении. Подлинность проверяют по источнику и обстоятельствам получения

СПОРНО

Хватит ли добровольной модели

для материалов, воспроизводящих облик или голос конкретного человека, обсуждается обособленный обязательный режим

Штрафы за немаркированный ИИ-контент остались проектом

Санкции отклоненного проекта КоАП и защита добросовестных

Privacy Advocates

10-50 тыс. ₽

граждане

по проекту № 1069331-8

100-200 тыс. ₽

должностные лица

по проекту № 1069331-8

200-500 тыс. ₽

юридические лица

по проекту № 1069331-8

ПРОЕКТЫ № 1069302-8 И 1069331-8

Штраф шел в паре с маркировкой

первый проект вводил видимую надпись и машиночитаемую метку для синтетического видео, второй штрафовал за их отсутствие

Злонамеренные

обман, вымогательство, клевета, порнография с чужим лицом

vs

Легитимные

кино, реклама, образование: разделение защищает невиновных от преследования

Итог: проект КоАП отклонен 10.06.2026, ст.11 закона 243-ФЗ санкций не устанавливает. Норм о синтетике в рекламе нет, претензию предъявят по общим правилам о введении в заблуждение

Мир регулирует дипфейки от запретов до фетв и гайдлайнов

Глобальный ландшафт: семь моделей регулирования синтетического контента

Privacy Advocates

СТРАНА	МОДЕЛЬ	СУТЬ ПОДХОДА
Италия	комплексный закон об ИИ	уголовная ответственность за вред от дипфейков, защита авторских прав, согласие родителей для детей до 14 лет
ЕС	прозрачность	ст.50 AI Act с 02.08.2026: раскрытие дипфейков и машиночитаемая маркировка синтетического контента
Великобритания	давление на платформы	угроза многомиллиардных штрафов за генерацию противоправного контента
Казахстан	этико-религиозный	фетва Духовного управления: злонамеренные дипфейки признаны харамом
Сингапур	рекомендательный	оценка киберрисков для финсектора, гайдлайны по борьбе с обходом биометрии
Индонезия	жесткая блокировка	запрет чат-ботов из-за угрозы эротических дипфейков
Россия	рамочный закон	закон об ИИ 243-ФЗ: добровольная пометка с 01.03.2027, остальное по общим нормам о ПД, изображении и ответственности

Суд признал дипфейк-сайт незаконным по иску Роскомнадзора

Таганский районный суд г. Москвы, дело 2-1452/2026: ИИ-контент с изображением человека без согласия незаконен

Privacy Advocates

04.06.2026

ТАГАНСКИЙ СУД

Иск Роскомнадзора удовлетворен

ответчик - иностранный регистратор домена NameSilo, установлен по whois, рассмотрено в его отсутствие

13.08.2026

МОТИВИРОВКА

Изображение - это ПД

распространение ИИ-материалов по фото и видео гражданина требует ч.1 ст.6 и ч.1 ст.10.1 152-ФЗ

после вступления

СТ.15.5 149-ФЗ

Реестр нарушителей

решение - основание для включения страницы в реестр нарушителей прав субъектов ПД

Тот же суд и тот же ответчик

по делу 02-0901/2026 признаны незаконными сбор и распространение ПД граждан на сайте того же регистратора: данные документов, СНИЛС, ИНН, фото

Вывод: синтетический контент на основе изображения реального человека требует согласия на распространение или иного основания, иначе страницу блокируют через реестр нарушителей

Платформы и медиа ставят фильтры раньше закона

Саморегулирование: доверие аудитории, ограничения доступа к генерации и детекторы

Privacy Advocates

Медиа

Трансформация медиа

баланс между автоматизацией производства и доверием аудитории: позиция Газпром-медиа

Модели

Ограничения под капотом

платный доступ к генерации как инструмент контроля: реакция Илона Маска и xAI

Рынок

Собственные детекторы

бизнес внедряет распознавание подделок, крупные маркетплейсы заявляют о высокой точности детекторов

ПРАКТИКА

Дипфейк-ролик охраняется как произведение

суды по делу А40-200471/2023 признали подмену лица инструментом монтажа, а не способом создания, и защитили права на ролик. Суд по интеллектуальным правам 19.08.2024 оставил решения в силе

- формула суда описывает операцию с исходной съемкой и не переносится на синтез голоса и материал без исходника
- проверку прав на исходник и обстоятельств получения материала ведет тот, кто его использует

Регулировать надо вред от дипфейка, а не технологию синтеза

Выводы раздела: баланс между чрезмерным регулированием и технологической вседозволенностью

Privacy Advocates

БАЛАНС

Точка равновесия

чрезмерное регулирование грозит преследованием добросовестных разработчиков и пользователей, технологическая вседозволенность - массовым мошенничеством. Точку равновесия ищут по индексу атрибутивности данных: насколько материал связан с конкретным человеком

Технологический нейтралитет

сама технология синтеза не преступна, наказывать следует за незаконную выгоду и реальный вред

Синергия мер

адекватные правовые рамки без загромождения УК и непрерывный технологический аудит

Взгляд в будущее

метрики атрибутивности для автоматической оценки легитимности синтетических данных в гибридных средах

Режим ПД уже работает

материал с узнаваемым обликом или голосом остается ПД, пометка подлинности не доказывает, риск несет тот, кто материал использует

Для DPO: проект с синтезом проверяют по четырем слоям: ПД, изображение гражданина, авторские и смежные права, осведомленность адресата, и собирают разрешения по каждому

ЧАСТЬ

VII

Риски, защита и инциденты

Как оценить риск, защитить ПД и пережить утечку

26 Управление прайваси-рисками
27 Защита ПД и СЗПД
28 Инциденты с ПД

26

Управление прайваси-рисками

Как оценить риск обработки ПД и принять решение, которое можно доказать

- 26.1 Риск-мышление
- 26.2 Оценка вреда и принципы
- 26.3 Алгоритм в три шага
- 26.4 Меры и доказуемость

Раздел на сайте
privacy-advocates.ru/pd/rsk

26.1

Риск-мышление

- Выиграть или не проиграть
- Как это выглядит в организации
- Прайваси-риск не сводится к угрозам безопасности
- Вред возникает, когда данные вырывают из контекста

Выиграть или не проиграть

Две крайности отношения к данным и прагматичный путь между ними

Privacy Advocates

ДАТА-ОПТИМИЗМ

Игра на победу, максимизация выгоды

Данные как новая нефть, чем их больше, тем больше ценности

Михаил Мишустин, премьер-министр РФ, 12.03.2020

- ✓ аналитика, персонализация и обучение ИИ
- ✗ накопленный объем умножает цену утечки

ДАТА-ПЕССИМИЗМ

Игра на избегание неудач, минимизация ущерба

Данные как токсичный материал, чем раньше их уничтожить, тем меньше уязвимость

Милош Вагнер, замруководителя РКН, 20.06.2023

- ✓ меньше поверхность утечки и санкций
- ✗ бизнес теряет ценность данных

ДАТА-ПРАГМАТИЗМ

Риск-ориентированный подход

- Классический privacy-комплаенс
- Бережливая обработка данных
- Технологии защищенной обработки данных

Как это выглядит в организации

Три опоры дата-прагматизма и DPO на страже рисков



Башня комплаенса
документы, роли и процессы, ответы субъектам и регулятору

Остров бережливой обработки
меньше данных и доступов, меньше территория для защиты

Мост ТЗОД
ценность данных доступна без их раскрытия

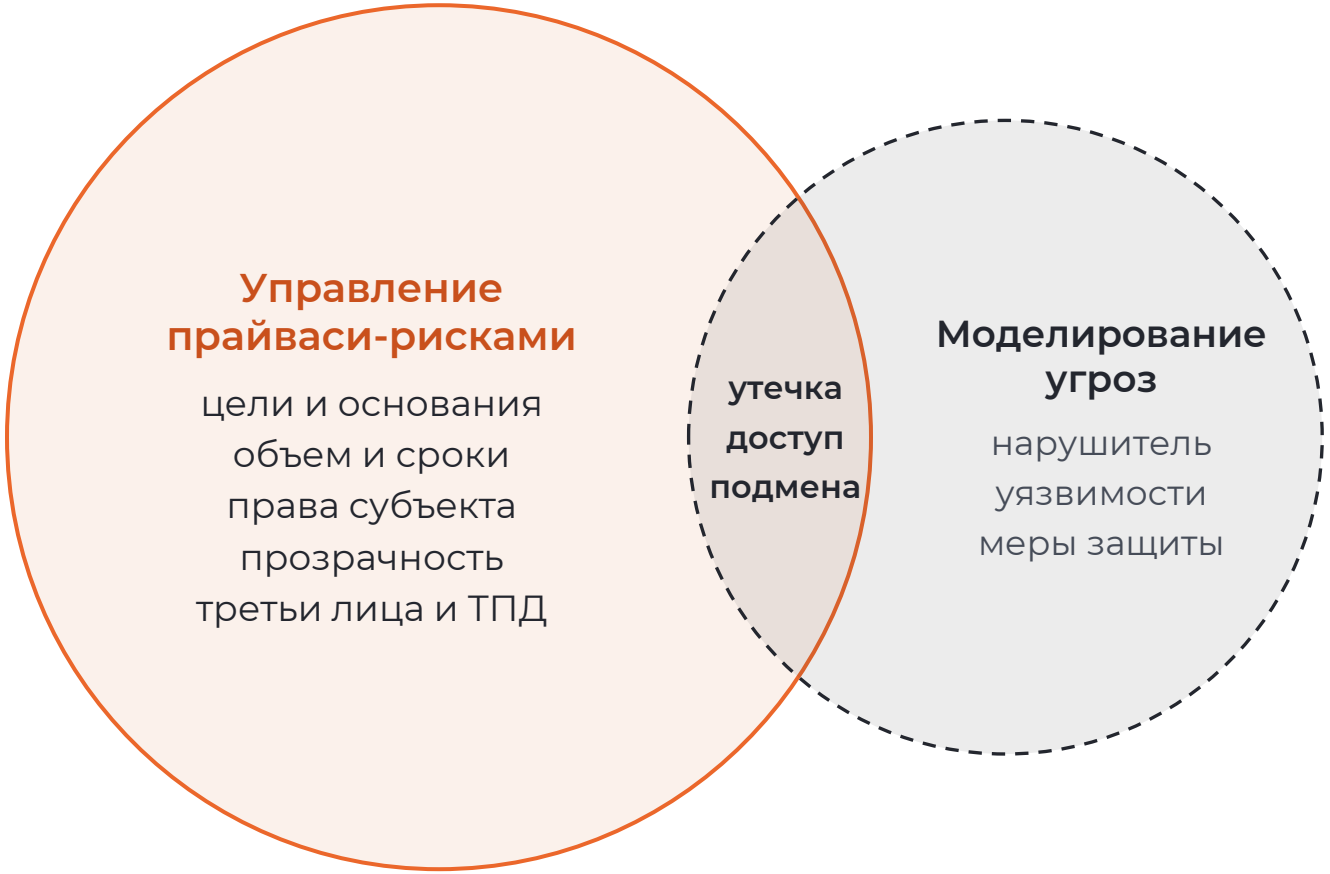
Страж на башне, DPO
замечает риски заранее и управляет ими

Регуляторно-нормативный ров окружает все, и каждая опора строится с учетом его требований

Прайваси-риск не сводится к угрозам безопасности

Где заканчивается управление рисками и начинается моделирование угроз

Privacy Advocates



КОМУ ГРОЗИТ РИСК

Субъекту ПД

Вред правам и интересам, его степень оценивается по приказу РКН № 178

Оператору

Санкции, убытки и потеря доверия, а с 30.05.2025 и оборотные штрафы за повторную утечку

Риск оценивают для обеих сторон, иначе решение будет однобоким

Эта часть. Стоит ли обрабатывать, в каком объеме и на каких условиях. **Следующая часть.** Как нарушитель доберется до данных и какие меры защиты нужны

Вред возникает, когда данные вырывают из контекста

У каждого человека несколько "я": для работы, друзей, родных и личной жизни

Privacy Advocates

Человек ведет себя по-разному в зависимости от контекста. Если данные из разных контекстов объединить, он больше не может разделять роли, предназначенные для разных людей

Работа

профиль в профессиональной сети: должность, опыт, деловые контакты

Друзья

соцсети с шутками, праздниками и спорами

Семья

фото детей, домашние события, адрес

Личная жизнь

приложения знакомств и то, что человек показывает только там

Правило: сводить в одну базу данные из разных источников и для разных целей без нужды нельзя: закон запрещает объединять базы с несовместимыми целями (ч.3 ст.5 152-ФЗ)

Регулятор уже мыслит рисками

Риск-ориентированный надзор, оценка вреда и санкции по масштабу утечки

Privacy Advocates

КАТЕГОРИЯ РИСКА ОПЕРАТОРА

- Высокий
- Значительный
- Средний
- Умеренный
- Низкий

С 01.07.2021 Роскомнадзор относит операторов к одной из пяти категорий риска по ПП № 1046, критерии переписаны ПП № 1286 от 27.08.2025

ОЦЕНКА ВРЕДА СУБЪЕКТУ



Оценка вреда обязательна для каждого оператора, степень определяется по **приказу РКН № 178 от 27.10.2022**, п.5 ч.1 ст.18.1 152-ФЗ

САНКЦИИ

до 500 млн ₽

оборотный штраф за повторную утечку, ст.13.11 КоАП с 30.05.2025

- Штраф за первую утечку зависит от числа субъектов и категорий ПД
- Незаконные сбор, хранение, использование и передача компьютерной информации с ПД криминализованы ст.272.1 УК РФ

Вывод. Риск-ориентированный подход уже встроен в регулирование, и у компании должна быть своя, документированная оценка

26.2

Оценка вреда и принципы

- Оценка вреда и DPIA
- Оценку вреда субъектам проводит каждый оператор
- Акт оценки вреда оператор во многом строит сам
- Шесть принципов риск-менеджмента ПД

Оценка вреда и DPIA

Российский обязательный минимум и европейская оценка воздействия на защиту ПД

Privacy Advocates

	РОССИЯ, ОЦЕНКА ВРЕДА п.5 ч.1 ст.18.1 152-ФЗ, приказ РКН № 178		ЕВРОСОЮЗ, DPIA ст.35 и ст.36 GDPR
Когда	всегда, оценка обязательна для каждого оператора	Когда	если обработка может повлечь высокий риск для прав и свобод людей
Что оценивают	степень вреда субъекту (высокая, средняя, низкая) по ситуациям из приказа № 178	Что оценивают	конкретную операцию, ее необходимость, пропорциональность, риски и меры
Результат	акт оценки вреда	Результат	отчет DPIA с мерами, его пересматривают при изменении риска
Высокий риск	отдельной процедуры нет, меры оператор выбирает сам	Высокий риск	консультация с надзорным органом до начала обработки

Вывод. Акт оценки вреда закрывает формальное требование, а решение о мерах дает оценка риска каждого процесса, по логике она ближе к DPIA

Оценку вреда субъектам проводит каждый оператор

Степени вреда по приказу Роскомнадзора от 27.10.2022 № 178

Privacy Advocates

Степень вреда по приказу № 178

Высокая

- биометрия вне случаев, прямо установленных законом
- спецкатегории вне случаев, прямо установленных законом
- ПД несовершеннолетних в (пред)договорных отношениях вне прямых указаний закона
- обезличивание, в том числе для исследований, вне п.9 ч.1 ст.6 152-ФЗ
- поручение обработки ПД граждан РФ иностранному лицу
- сбор ПД с использованием баз за пределами РФ

Средняя

- распространение ПД вне прямых указаний закона, в том числе в результате инцидента
- обработка в дополнительных целях, отличных от первоначальной цели сбора
- продвижение товаров прямыми контактами по чужой базе ПД
- согласие через простую веб-форму (click-wrap) на сайте
- согласие в отношении (не)определенного круга лиц в несовместимых между собой целях

Низкая

- ведение общедоступных источников ПД по ст.8 152-ФЗ
- назначение ответственным за организацию обработки ПД лица не из штата оператора

Правило: при нескольких основаниях выбирают наиболее высокую степень, а если ни один вид обработки не подходит, по устной позиции Роскомнадзора в акте пишут, что степень вреда не выявлена

Акт оценки вреда оператор во многом строит сам

Что обязательно указать в акте и что Роскомнадзор оставил на усмотрение оператора

Privacy Advocates

Акт оценки вреда

Обязательные реквизиты

- наименование или ФИО и адрес оператора
- дата издания акта и дата проведения оценки
- ФИО, должности и подписи тех, кто проводил оценку
- степень вреда, а из нескольких выбирают наиболее высокую
- перечень случаев причинения вреда закрытый

Роскомнадзор

Что решает оператор

- случаи проведения оценки, по видам деятельности и по каждой ИСПД или в совокупности
- методику, объект, причины, срок или период оценки
- состав и порядок работы комиссии
- соотношение вреда и принимаемых мер
- вопросы безопасности ПД приказ не затрагивает, это компетенция ФСБ и ФСТЭК

Пробелы: срок хранения акта, основания и периодичность пересмотра приказ не задает, поэтому их закрепляют в локальном акте. Сведения об ИСПД в акте не обязательны (Управление по Камчатскому краю, 14.12.2023)

Шесть принципов риск-менеджмента ПД

Контроль рисков с учетом риск-толерантности и ожиданий заинтересованных сторон

Privacy Advocates

Не навреди

Не снижать риски ПД за счет роста иных рисков

Документы

Нет документированной информации, нет и управления рисками

Срок годности

Оценка устаревает вместе с факторами риска, ее пересматривают



Активное взаимодействие

Вовлекать в оценку и обработку рисков заинтересованные стороны

Своя методика

Универсальной методики нет, она должна быть специфичной и удобной

Чем проще, тем лучше

Методика и результат понятны и воспроизводимы

Те, кто пренебрегает документами, - воск в руках тех, кто документами не пренебрегает

26.3

Алгоритм в три шага

- Алгоритм в три шага
- Как ставить оценки и искать отклонения
- Уровень риска как координата процесса
- От оценки к плану реагирования

Алгоритм в три шага

Анализ обработки, выявление отклонений, управление рисками

Схема риск-менеджмента
скачать

Privacy Advocates

1 Анализ обработки

дает виктимность

- 1.1 Статус лица в отношении ПД
- 1.2 Цель обработки
- 1.3 Чувствительность ПД
- 1.4 Источники получения
- 1.5 Категории субъектов
- 1.6 Участие третьих лиц
- 1.7 Трансграничная передача
- 1.8 Масштаб обработки
- 1.9 Сценарии обработки
- 1.10 Заметность (множитель)

2 Выявление отклонений

дает критичность

- 2.1 Цели и пропорциональность
- 2.2 Основания обработки
- 2.3 Передача ПД третьим лицам
- 2.4 Жизненный цикл ПД
- 2.5 Взаимодействие с субъектами
- 2.6 Взаимодействие с органами
- 2.7 Обучение персонала
- 2.8 Отклонения и инциденты
- 2.9 Безопасность обработки
- 2.10 Руководство и учет

3 Управление рисками

- 3.1 Оценка уровня риска
- 3.2 Выбор метода реагирования
- 3.3 Определение мер
- 3.4 Планирование мер

Методика и калькулятор

Как ставить оценки и искать отклонения

Шкала из трех уровней для шага 1 и цена санкций для шага 2

Пособие к калькулятору
скачать

Privacy Advocates

ШАГ 1. ТРИ УРОВНЯ ОЦЕНКИ ФАКТОРА

1.5 Категории субъектов

равноправная сторона, не зависят от оператора

более слабая сторона, зависят от оператора

недееспособные или ограниченно дееспособные

1.8 Масштаб обработки

нерегулярная и затрагивает мало субъектов

регулярная или затрагивает много субъектов

регулярная и затрагивает много субъектов

ШАГ 2. ЦЕНА САНКЦИЙ ПО ОБЛАСТЯМ КОНТРОЛЯ

2.4	**Жизненный цикл ПД**	⚡⚡⚡
2.9	**Безопасность обработки**	⚡⚡⚡
2.2	Основания обработки	⚡⚡
2.3	Передача ПД третьим лицам	⚡⚡
2.8	Отклонения и инциденты	⚡⚡
2.1	Цели и пропорциональность	⚡
2.5	Взаимодействие с субъектами	⚡
2.6	Взаимодействие с органами	⚡
2.7	Обучение персонала	⚡
2.10	Руководство и учет	⚡

сначала опишите процесс обработки, потом оценивайте

масштаб анализа выбирайте сами, от процесса маркетинга до одного сайта

требования ищите в приказе РКН № 253, ПП № 1046, ПП № 24 и отраслевых НПА

соблюдение проверяйте через чек-листы и закрытые вопросы

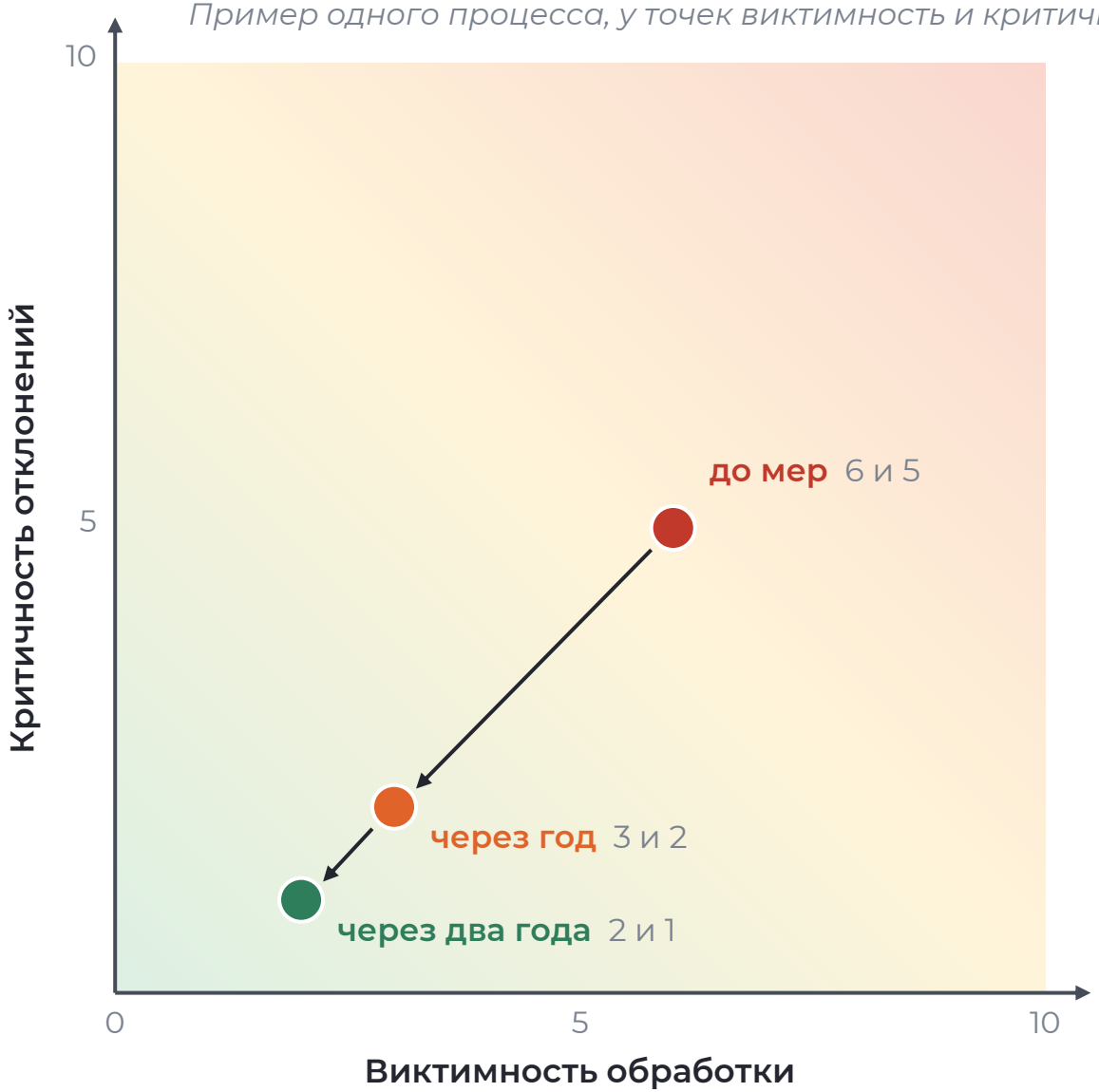
Чек-лист контролей

Уровень риска как координата процесса

Две оценки дают точку, повторные оценки показывают динамику

Privacy Advocates

Пример одного процесса, у точек виктимность и критичность



Виктимность обработки
сумма оценок 1.1-1.9, умноженная на 1.10
насколько процесс уязвим и заметен

Критичность отклонений
сумма оценок выявленных отклонений 2.1-2.10
насколько процесс расходится с требованиями

Уровень риска
соотношение двух оценок
чем дальше точка от начала координат, тем выше риск

Оценки пересматривают регулярно, риск-факторы меняются во времени

Риск-толерантность определяют вместе с владельцем процесса обработки и риска

От оценки к плану реагирования

Четыре метода, пять видов мер и три вопроса плана

Privacy Advocates

ЧЕТЫРЕ МЕТОДА

Снижение
меры уменьшают виктимность или критичность

Принятие
остаточный риск в пределах риск-толерантности

Отказ
прекратить процесс или его часть

Передача
договор и страхование, но перед субъектом отвечает оператор

МЕРЫ И ПЛАН, ТИПОВОЕ РАСПРЕДЕЛЕНИЕ

Вид меры	Кто делает	Когда
Корректировка отношений с субъектами	владелец процесса, DPO	быстро
Корректировка отношений с третьими лицами	закупки, юристы	быстро
Корректировка внутренней документации	DPO	быстро
Минимизация процесса обработки	владелец процесса	долго
Изменение ИТ-систем и инфраструктуры	ИТ и ИБ	долго

Три вопроса плана **что делаем, кто делает, в какие сроки**

Остаточный риск после мер тоже оценивают и принимают решением владельца риска

26.4

Меры и доказуемость

- Бережливая обработка данных
- Технологии защищенной обработки данных
- Решение, которое можно доказать
- Мост к моделированию угроз

Бережливая обработка данных

Самая дешевая мера снижения риска по аналогии с бережливым производством

Privacy Advocates

Убираем из процесса все, что не добавляет ценности результату, но добавляет риск



ЧТО ДАЕТ КОМПАНИИ

Меньше цена утечки

меньше данных, меньше вероятность утечки и ответственности за нее

Дешевле ИТ и ИБ

меньше ресурсов на хранение, обработку и защиту

Privacy-имидж

добросовестные практики и соответствие ожиданиям регулятора

ПОДХОДЫ РКН К НАДЛЕЖАЩЕЙ ОБРАБОТКЕ ПД

01 минимизировать перечень собираемых и обрабатываемых ПД

02 хранить раздельно категории ПД, несовместимые по целям

03 держать ФИО и контакты отдельно от данных о взаимодействии с человеком

04 не копить ПД на всякий случай и не строить профили без необходимости

05 реже поручать обработку третьим лицам, поручение не снимает ответственность

Технологии защищенной обработки данных

ТЗОД снижают виктимность и сохраняют ценность данных для бизнеса

Privacy Advocates

ВЫЧИСЛЕНИЯ БЕЗ РАСКРЫТИЯ

Доверенные среды, TEE
обработка в защищенном анклаве процессора

Разделение секрета, SMPC
каждый видит только свою часть секрета

Федеративное обучение
модель едет к данным, а не данные к модели

Синтетические данные
свойства реальных данных без реальных людей

ИДЕНТИФИКАЦИЯ БЕЗ ЛИШНЕГО

Контекстные ID
номерок в гардеробе, снаружи по нему не найдут

Децентрализованные ID
показать только нужное, например 18+

Нулевое разглашение, ZKP
доказать факт, не раскрывая сам секрет

Геонеразличимость
вы где-то в парке, а не на этой скамейке

ГДЕ ПРИМЕНЯЮТ

кибербезопасность | обучение ИИ | аналитика данных | госсервисы

КЕЙС

Банк России одобрил МРС

В 2024 году банкам разрешили считать долговую нагрузку заемщика по поступлениям на его счета в других банках. Расчет идет на платформе счет-скоринга с совместными конфиденциальными вычислениями, без раскрытия банковской тайны

ПРАВОВОЙ СТАТУС

Закон не регулирует ТЗОД сами по себе, а ПД и тайны после их применения не меняют статус

Белая книга ТЗОД
Ассоциация больших данных и Privacy Advocates

Решение, которое можно доказать

Какие документы оставляет каждый шаг управления рисками

Privacy Advocates

шаг 1	приказ № 178	шаги 2 и 3.1	шаг 3.2	шаги 3.3 и 3.4	срок годности
Карточка процесса	**Акт оценки вреда**	**Отчет об оценке риска**	**Решение владельца риска**	**План мер**	**Дата пересмотра**
цели, состав ПД, субъекты, третьи лица и сценарии	степень вреда, обязателен для каждого оператора	виктимность, критичность, отклонения и уровень риска	метод реагирования и принятие остаточного риска	что делаем, кто делает, в какие сроки	когда и после каких изменений оценку обновят

ПРОВЕРКА ИЛИ ИНЦИДЕНТ

спросят не о том, был ли риск, а как вы его оценили, кто принял решение и что сделано по плану

С ЧЕГО НАЧАТЬ

пилот на двух-трех самых заметных процессах, весь цикл от карточки до плана мер

Мост к моделированию угроз

Что оценка прайваси-рисков передает дальше и что получает обратно

Privacy Advocates

Управление прайваси-рисками

стоит ли обрабатывать и на каких условиях

ПЕРЕДАЕМ →

- процессы и ИСПД с высоким уровнем риска, с них начинают моделирование
- категории и объем ПД и субъектов для уровня защищенности по ПП № 1119
- третьих лиц, обработчиков и ТПД, это границы и интерфейсы системы
- риск-толерантность владельца, то есть допустимый остаточный риск

ПОЛУЧАЕМ ОБРАТНО ←

- тип актуальных угроз и модель нарушителя, они уточняют оценку области 2.9
- меры защиты, они входят в план как изменение ИТ-систем

Моделирование угроз

как нарушитель доберется до данных и чем защититься

Один цикл, два взгляда. Риск-менеджмент решает, стоит ли обрабатывать, а модель угроз решает, как защитить то, что решили обрабатывать

Как эффективно управлять рисками обработки ПД?

Минимизируйте обработку ПД

КЛЮЧЕВЫЕ ВЫВОДЫ

- Прайваси-риск шире угроз безопасности, поэтому цели, основания, объем и права субъекта оцениваются наравне с защитой
- Регулятор уже мыслит рисками, это категории риска в надзоре, оценка вреда и штрафы по масштабу утечки
- Уровень риска складывается из виктимности обработки и критичности отклонений, и его регулярно пересматривают
- Самая дешевая мера снижения риска это минимизация обработки, а каждое решение о риске оставляет документ

27

Защита ПД и СЗПД

Определение ИСПД, угрозы, меры и СЗИ

27.1 Определение ИСПД

27.2 Угрозы и уровни защищенности

27.3 Создание СЗПД и роли

27.4 СЗИ и оценка эффективности

Раздел на сайте
privacy-advocates.ru/pd/szp

27.1

Определение ИСПД

- ИСПД определяют в два шага: сначала систему, затем ее оператора

ИСПД определяют в два шага: сначала систему, затем ее оператора

Алгоритм определения ИСПД и оператора ИСПД, версия 2.0

Privacy Advocates

ЭТАП	ВОПРОС	ДА	НЕТ
Ресурс	I. Обрабатываются ли с помощью ресурса ПД: сбор, получение, передача, хранение?	к вопросу II	не ИСПД
Ресурс	II. Из ПД в ресурсе обрабатываются только логины и пароли пользователей?	не ИСПД	ИСПД, к этапу 2
Лицо	III. Признает ли себя лицо оператором или обработчиком ПД в этой ИСПД?	к вопросу V	к вопросу IV
Лицо	IV. Есть ли у лица технический доступ к ПД, даже зашифрованным без ключа?	к вопросу V	не оператор ИСПД
Лицо	V. Владеет ли лицо на вещном праве техническими средствами с базой ПД?	к вопросу VI	пользователь ИСПД
Лицо	VI. Лицо лишь предоставляет свои технические средства под чужие базы ПД?	не оператор ИСПД	к вопросу VII
Лицо	VII. Заключен ли лицом договор на всестороннюю эксплуатацию ИСПД?	оператор - контрагент	оператор ИСПД

Ресурс

ИС, в том числе облачная, почта, мессенджер, ВКС, сетевой диск, сайт, мобильное приложение

Эксплуатация ИС

сопровождение ПО, оборудования и СЗИ, обучение, обслуживание, закупка, модернизация, обновление

27.2

Угрозы и уровни защищенности

- Каждый уровень защищенности добавляет новые требования

Каждый уровень защищенности добавляет новые требования

Что требует ПП-1119 на каждом уровне и от чего зависит уровень конкретной ИСПД

Анализ ПП № 1119
скачать

Privacy Advocates



Уровень задают

- тип актуальных угроз
- категория ПД: специальные, биометрические, общедоступные, иные
- сотрудники оператора или иные лица
- больше или меньше 100 тыс. субъектов

Правило: уровень устанавливают для каждой ИСПД отдельно, а при нескольких сработавших условиях берут самый строгий. При любом уровне оператор ИСПД определяет угрозы, оценивает эффективность мер до ввода системы, устанавливает правила доступа, регистрирует действия с ПД и контролирует меры

27.3

Создание СЗПД и роли

- Ответственному за безопасность ПД в ИСПД нужны полномочия
- Проект по защите ПД занимает около полугода
- Меры защиты ПД: что действует и что готовится

Ответственному за безопасность ПД в ИСПД нужны полномочия

Должностное лицо по п.14 ПП-1119: функции, кандидаты, санкции и выгоды назначения

Privacy Advocates

П.14 ПП-1119

Назначение обязательно с 3 уровня защищенности

работник оператора ИСПД отвечает за обеспечение безопасности ПД в информационной системе; при СКЗИ приказ ФСБ № 378 требует достаточных навыков

ФУНКЦИИ И ЗАДАЧИ

- **организация и координация** безопасности ПД в системах
- определение актуальных угроз
- организационные и технические меры защиты
- восстановление ПД после несанкционированного доступа
- правила доступа, регистрация и учет действий с ПД
- контроль принятых мер
- распорядительные документы по безопасности ПД
- **обнаружение, расследование и ликвидация** последствий инцидентов с ПД

Кандидаты

Из профильных подразделений

CISO или CIO, их заместители и ведущие специалисты подразделений ИБ и ИТ, либо DPO

Санкция

Ч.6 ст.13.12 КоАП

за неназначение и иные нарушения защиты информации: юрлицу 50-100 тыс. ₽, должностному лицу 10-50 тыс. ₽. В госорганах и НКО риски выше

Выгода

Ответственность концентрируется

снижается риск привлечения ЕИО при компьютерном инциденте, но от контроля за подчиненными руководителя это не освобождает

Проект по защите ПД занимает около полугода

Три этапа: результат каждого этапа становится исходными данными следующего

Privacy Advocates

1 Модель угроз ПД — 30 раб. дней

ИСХОДНЫЕ ДАННЫЕ

- реестр процессов и ИСПД
- опросник о применяемых СЗИ

РАБОТЫ

- анализ угроз безопасности ПД
- выявление актуальных угроз
- модель угроз по документам ФСТЭК

РЕЗУЛЬТАТ

модель угроз, при привлечении лицензиата ФСТЭК или ФСБ согласованная с ним

2 Меры защиты ПД — 30 раб. дней

ИСХОДНЫЕ ДАННЫЕ

- модель угроз

РАБОТЫ

- меры защиты ПД и устранения актуальных угроз
- техническое задание на СЗПД
- технический проект по документам ФСТЭК и ФСБ

РЕЗУЛЬТАТ

техническое задание и проект СЗПД: спецификация СЗИ и пояснительная записка

3 Закупка и внедрение СЗИ — 60+ раб. дней

ИСХОДНЫЕ ДАННЫЕ

- спецификация СЗИ из технического проекта

РАБОТЫ

- закупка СЗИ по спецификации
- внедрение и настройка, состав и сроки по договоренности

РЕЗУЛЬТАТ

СЗПД по документам ФСТЭК и ФСБ

Учесть: лицензиата оператор привлекает по выбору, свои системы вправе защищать сам и сам выбирает форму документа об угрозах (письмо ФСТЭК от 10.04.2025). До нового приказа состав мер задает приказ № 21

Меры защиты ПД: что действует и что готовится

Состав мер на 30.09.2026: базовые акты, документы ФСТЭК и ФСБ и проект замены приказа № 21

Privacy Advocates

АКТ	СТАТУС	ЧТО ЗАДАЕТ
ПП № 1119	действует	четыре уровня защищенности ПД и требования к каждому из них
Приказ ФСТЭК № 21	под отмену	состав и содержание мер, таблица базовых мер по уровням защищенности
Проект ФСТЭК № 169583	не принят	21 мероприятие и 17 групп технических мер без таблицы, состав мер в политике, показатель зрелости
Документы ФСТЭК 2026 года	ориентир	меры в ИС (12.04.2026), методика зрелости (07.08.2026), разъяснение о внеплановой оценке (24.08.2026)
Приказ ФСТЭК № 117	госсистемы	в ред. № 137 с 01.09.2026, новый порядок расчета К(зи) и У(зи) подрядчиков с 01.03.2027
Приказы ФСБ № 378 и № 321	СКЗИ	№ 378 для ИСПД, № 321 от 22.08.2026 для систем госорганов: четыре случая обязательной криптозащиты

Подготовка: пока проект не принят, меры ведут в двух колонках: код меры приложения к приказу № 21 и направление из перечней проекта. Тогда переход сведется к перемаркировке, а не к пересборке набора

27.4

СЗИ и оценка эффективности

- СЗПД собирают из мер, а средства подбирают под меры

СЗПД собирают из мер, а средства подбирают под меры

Организационно-технические меры, механизмы ОС и дополнительные программные средства

Privacy Advocates

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРЫ

- резервное копирование
- изоляция участков памяти
- уничтожение остаточных данных
- контроль целостности
- смена паролей
- ограничение сетевых служб и протоколов

ПРОГРАММНЫЕ СРЕДСТВА ОС

- защита от исследования, модификации и запуска
- предупреждение об опасных действиях
- разграничение полномочий, регистрация, контроль
- идентификация и аутентификация
- резервное копирование

ДОПОЛНИТЕЛЬНЫЕ ПРОГРАММНЫЕ СРЕДСТВА

Криптографические

абонентское и канальное шифрование, шифрование паролей, стеганография, электронная подпись, VPN

Защита от вредоносных программ

контроль целостности, обнаружение вредоносных программ, тестирование, утилиты восстановления

Сетевые

тестирование сетей и программ, обнаружение атак, межсетевые экраны

Порядок: сначала меры, затем средства с нужными функциями, штатные механизмы ОС не дублируют. Сертифицированные СЗИ нужны против актуальных угроз, СКЗИ - для незащищенных каналов и носителей. Эффективность оценивают до ввода ИСПД

28

Инциденты с ПД

Квалификация утечки, уведомления и план реагирования

28.1 Понятие и квалификация инцидента

28.2 Стратегия реагирования

28.3 Уведомления и ожидания РКН

28.4 Тактика, PR и компенсации

28.5 План реагирования и плейбук

28.6 Ответственность и практика по утечкам

Раздел на сайте
privacy-advocates.ru/pd/inc

28.1

Понятие и квалификация инцидента

- Инцидентом считают любое нарушение безопасности ПД
- Закон знает три дефиниции утечки, и они не совпадают
- Роскомнадзор отделяет инциденты от рядовых событий
- Принадлежность утечки оператору подтверждают пять признаков

Инцидентом считают любое нарушение безопасности ПД

Общепринятое понимание: конфиденциальность, целостность и доступность при любой обработке

Privacy Advocates

ОПРЕДЕЛЕНИЕ

Инцидент с ПД

любое нарушение **конфиденциальности, целостности и (или) доступности** ПД в процессе автоматизированной и (или) неавтоматизированной обработки

ТИПИЧНЫЕ ПРИМЕРЫ

- взлом учетной записи пользователя
- взлом информационной системы или базы с ПД
- неправильное уничтожение ПД на устройстве
- неправильное уничтожение документа с ПД
- утеря устройства с ПД
- утеря документа с ПД
- неверно направленное письмо с ПД
- несанкционированный доступ к ПД
- несанкционированное копирование ПД
- несанкционированная публикация ПД

Закон знает три дефиниции утечки, и они не совпадают

Инцидент по 152-ФЗ, компьютерный инцидент и утечка по КоАП

Privacy Advocates

ПРИЗНАК	ИНЦИДЕНТ, Ч.3.1 СТ.21 152-ФЗ	КОМПЬЮТЕРНЫЙ ИНЦИДЕНТ, Ч.12 СТ.19 152-ФЗ	УТЕЧКА, Ч.12-18 СТ.13.11 КОАП
Действие	передача: предоставление, распространение, доступ	передача: предоставление, распространение, доступ	передача: предоставление, распространение, доступ
Предмет	ПД	ПД	информация, включающая ПД и (или) идентификаторы в ИСПД
Характер	неправомерная или случайная	неправомерная	неправомерная
Причина или последствие	повлекла нарушение прав субъектов ПД	произошла в результате компьютерной атаки	произошла в результате действий или бездействия оператора
Кого уведомить	Роскомнадзор	ФСБ через ГосСОПКА	отдельной обязанности нет

Следствие: одно событие бывает сразу инцидентом для Роскомнадзора, компьютерным инцидентом для ГосСОПКА и утечкой для КоАП, поэтому квалификацию ведут по всем трем дефинициям

Роскомнадзор отделяет инциденты от рядовых событий

Что считается инцидентом по приказу № 187 и по позиции регулятора

Privacy Advocates

Инцидент

Является инцидентом

- база ПД доступна неограниченному кругу лиц в результате неправомерной или случайной передачи ПД (приказ Роскомнадзора от 14.11.2022 № 187)
- несанкционированный доступ внешнего пользователя к базе ПД
- несанкционированный доступ из-за уязвимостей ПО системы
- неправомерное копирование базы ПД
- копия базы ПД, актуальная или скомпрометированная ранее, доступна в интернете
- получено сообщение с угрозой раскрыть базу ПД

vs

Не инцидент

Не является инцидентом

- несанкционированный доступ внутреннего пользователя к базе ПД без копирования
- случайное уничтожение базы ПД внутренним пользователем
- подозрительная активность пользователя системы

Принадлежность утечки оператору подтверждают пять признаков

Как Роскомнадзор связывает инцидент с конкретным оператором

Privacy Advocates

1

Признание оператора

оператор сам подтверждает факт инцидента в уведомлении или в ходе проверки

2

Совпадение с ИСПД

содержание утечки совпадает с данными системы, которую исследует Роскомнадзор: конкретные значения, набор полей

3

Обстоятельства

из деталей следует, что данные относятся к оператору: названо его наименование или характер деятельности предполагает такие данные

4

Скриншоты

данные совпадают со скриншотами, которые представил оператор или получил регулятор в ходе проверочного мероприятия

5

Связанный ресурс

данные размещены на ресурсе, связанном с оператором, например на его собственном сайте

Практический вывод: отрицание утечки при совпадении хотя бы части признаков только ухудшает позицию оператора в проверке и в суде

Как не надо реагировать на утечку

Ироничная схема типовых отговорок, которые не работают

Privacy Advocates

1. **Утечка произошла у вас?**
   нет - берите попкорн и наблюдайте
2. **Об утечке написали в СМИ?**
   нет - снова попкорн
3. **Да - выберите отговорку**
   можно несколько, а затем снова попкорн

Это не у нас, а у подрядчика

Это устаревшие, неактуальные данные

Это повтор прошлогодней утечки

Это провокация и происки конкурентов

Это не ПД, они обезличены

Пресс-релиз все стерпит

На деле: обработчик не снимает ответственности с оператора, повторная утечка наказывается оборотным штрафом, а обезличенные данные остаются ПД

Пирамида признания: от отрицания до разговора с пострадавшими

Как компании публично реагировали на утечки

Privacy Advocates



- **Признание и коммуникация** — подтверждение от своего лица и **коммуникация с пострадавшими** [Яндекс, ВкусВилл]
- **Признание от своего лица** — подтверждение утечки от своего лица [DNS]
- **Признание через прессу** — подтверждение утечки через СМИ [Спортмастер, СДЭК, Whoosh]
- **Признание без ответственности** — подтверждение утечки с отказом от ответственности [Альфастрахование]
- **Отрицание** — отрицание утечки, версия о компиляции старых баз [Сбер]
- **Активный отказ** — отказ от принадлежности утечки и попытки пресечь обсуждение [Geekbrains]

28.2

Стратегия реагирования

- Стратегия реагирования: не проиграть или выиграть
- Рабочая группа по реагированию собирается из семи ролей
- Управляем утечкой: думаем медленно, решаем быстро

Стратегия реагирования: не проиграть или выиграть

Две игры с разной целью и разной ценой ошибки

Privacy Advocates

Игра на избегание неудач

Минимизация издержек от утечки

- ограниченное раскрытие и юридически выверенные формулировки
- фокус на соблюдении сроков уведомлений и защите в проверке
- цель - минимальный штраф и ущерб репутации

vs

Игра на победу

Максимизация пользы от утечки

- проактивная коммуникация с субъектами, партнерами и регулятором
- демонстрация принятых мер и инвестиций в защиту
- цель - сохранить и укрепить доверие, превратить кризис в аргумент

Решение: выбор игры делают в первые дни инцидента, и от него зависят тактика, бюджет и состав рабочей группы

Рабочая группа по реагированию собирается из семи ролей

Кого звать в команду с первого дня

Privacy Advocates

Юрист

квалификация, сроки, позиция в проверке и суде

Прайвасист

оценка вреда субъектам, уведомления, связь с регулятором

Бизнес

решения о ресурсах, компенсациях и коммуникации

ИТ и ИБ

локализация инцидента, расследование, технические меры

PR

позиция компании для СМИ, клиентов и партнеров

Консультант

внешняя экспертиза и независимый взгляд

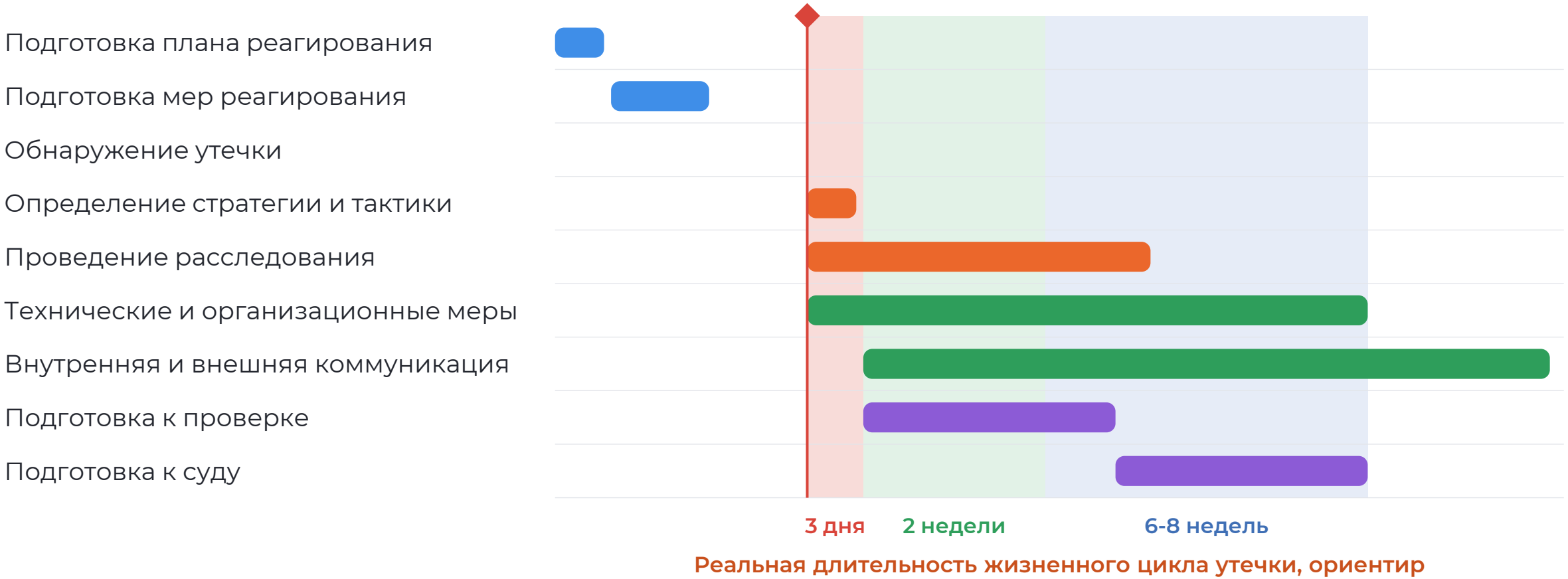
Советник консультанта

узкая экспертиза под конкретный кейс

Управляем утечкой: думаем медленно, решаем быстро

Реальный жизненный цикл утечки длиннее, чем кажется в первый день

Privacy Advocates



28.3

Уведомления и ожидания РКН

- Об утечке уведомляют до трех адресатов
- Роскомнадзор ждет два уведомления: через 24 и через 72 часа
- По утечке Роскомнадзор сначала запрашивает документы

Об утечке уведомляют до трех адресатов

Кто выявляет инцидент, по какому акту и куда направляют уведомления

Privacy Advocates

Реагирование на инцидент с ПД

Неправомерная или случайная передача ПД, нарушившая права субъектов	Компьютерный инцидент, повлекший неправомерную передачу ПД	Раскрытие ПД в составе банковской тайны или защищаемой информации
выявить может оператор, Роскомнадзор или иное лицо	выявляет оператор ИСПД	выявляет кредитная или некредитная финансовая организация
Приказ РКН № 187: о факте инцидента (24 часа) и о результатах расследования (72 часа)	**Приказ ФСБ № 77:** об обнаружении (24 часа), о результатах (72 часа) через портал РКН. Госсистемы с 01.09.2026 по приказу № 297, КИИ с 30.01.2026 по № 547 (3 часа по значимому объекту)	**СТО БР БФБО-1.5-2023:** об обнаружении (24 часа, 3 часа при ГОСТ Р 57580.1-2017) и о результатах расследования (30 дней)
Роскомнадзор	**ФСБ**	**Банк России**
портал pd.rkn.gov.ru/incidents/form	портал РКН, если нет соглашения с НКЦКИ; ГосСОПКА для ЗОКИИ или по соглашению с НКЦКИ	ФинЦЕРТ или ГосСОПКА, а также портал РКН

За неуведомление: штраф до 3 млн ₽ по ч.11 ст.13.11 КоАП, а при оборотном штрафе за утечку это отягчающее обстоятельство

Роскомнадзор ждет два уведомления: через 24 и через 72 часа

Содержание уведомлений по ч.3.1 ст.21 152-ФЗ, оба срока считают от выявления

Privacy Advocates



Сведения об инциденте

- дата и время выявления инцидента
- предполагаемые причины, например несанкционированный доступ внешнего пользователя
- характеристики ПД: категории, субъекты, примерное число записей, актуальность базы, период сбора
- предполагаемый вред правам субъектов
- принятые меры по устранению последствий
- дополнительные сведения (источник информации, ссылки на ресурсы) и материалы о принятых мерах
- контакты лица, уполномоченного взаимодействовать с Роскомнадзором

Результаты внутреннего расследования

- причины инцидента и нанесенный вред
- информационная система, к которой получен доступ
- дополнительные меры по итогам расследования
- решение оператора о проведении расследования с реквизитами
- сведения о лицах, действия которых стали причиной инцидента

Важно: отсчет идет с момента выявления инцидента оператором, Роскомнадзором или иным заинтересованным лицом

По утечке Роскомнадзор сначала запрашивает документы

Первичный запрос сведений по инциденту при внеплановой проверке

Privacy Advocates

Запрос Роскомнадзора об инциденте

Сведения об операторе

- документ о назначении уполномоченного представителя оператора
- устав оператора - юридического лица

Локальные акты

- политика оператора в отношении обработки ПД
- акты о предотвращении, выявлении и устранении последствий нарушений законодательства о ПД
- документы о правовых, организационных и технических мерах безопасности ПД

Сведения об ИСПД

Описание ИСПД

- наименование, назначение и адрес размещения БД
- категории субъектов, перечень ПД и действий с ними
- инструкции и документы по функционалу
- наименование и версии ПО, места нахождения компонентов

Сопровождение

- технологическое и информационное сопровождение, в т.ч. договоры с сервис-провайдерами

Совет: по утечке чаще ведут административное расследование (ст.28.7 КоАП) и истребуют сведения с ответом за 3 дня (ч.2 ст.26.10). Состав запроса зависит от инцидента, поэтому пакет документов готовят заранее

28.4

Тактика, PR и компенсации

- Стратегию начинают с оценки содержания инцидента
- Реакция на инцидент: обстоятельства в пользу оператора
- Тактика до инцидента: меры, которые потом защитят
- Тактика во время инцидента: расследовать, уведомить, изолировать

Стратегию начинают с оценки содержания инцидента

Обстоятельства, которые снижают тяжесть последствий

Privacy Advocates

СОДЕРЖАНИЕ ИНЦИДЕНТА

Что смягчает оценку

Эти факторы стоит зафиксировать документально с первого дня

Малозначительность

небольшой масштаб с точки зрения числа затронутых субъектов ПД и идентификаторов

Нет чувствительных данных

затронуты ПД без специальных, биометрических и иных чувствительных категорий

Нет уязвимых групп

субъекты не относятся к социально незащищенным группам населения

Кратковременность

кратковременный доступ третьих лиц из-за технического сбоя или случайности

NDA

непреднамеренный доступ к ПД третьих лиц, связанных с оператором соглашением о конфиденциальности

Третьи лица

действия или бездействие обработчиков либо действия злоумышленников

Сложность атаки

высокопрофессиональный характер кибератаки, специфическое ПО, изощренные техники

Реакция на инцидент: обстоятельства в пользу оператора

Что учитывают при выборе позиции и наказания

Privacy Advocates

Об операторе

- инцидент произошел впервые, оператор ранее не привлекался к ответственности
- признание вины и раскаяние оператора
- неустойчивое материальное положение оператора
- статус субъекта малого и среднего предпринимательства
- статус социально ориентированной некоммерческой организации

Об инциденте и обстановке

- нет жалоб, претензий и исков субъектов в связи с инцидентом
- вред субъектам оценен как средний по абз.2 п.2.2 приказа Роскомнадзора № 178
- напряженная геополитическая обстановка и рост хакерских атак на российские компании

Практика: арбитражные суды учитывали их при замене штрафа предупреждением в 2025 году, но с 2026 года мировые судьи дают предупреждение редко, а при объемных утечках апелляция считает его недопустимым

Тактика до инцидента: меры, которые потом защитят

Подготовка, которая становится доказательством

Privacy Advocates

01

Меры защиты

реализация необходимых и достаточных правовых, организационных и технических мер защиты ПД

02

Оценка соответствия СЗИ

применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия

03

Контроль мер

контроль за мерами по обеспечению безопасности ПД, в том числе у лиц, привлеченных к обработке

Почему это важно: в делах о хакерских атаках суды требуют от оператора доказать, какие меры он принял, поэтому документы о мерах готовят до инцидента

Тактика во время инцидента: расследовать, уведомить, изолировать

Организационные и технические меры в острой фазе

Privacy Advocates

1. внутреннее расследование или служебная проверка для выявления причин
2. своевременное и надлежащее уведомление Роскомнадзора
3. взаимодействие с Роскомнадзором в ходе проверки
4. обращение в правоохранительные органы, ФСБ и (или) НКЦКИ, признание оператора потерпевшим, возбуждение уголовного дела
5. оповещение заинтересованных лиц, включая субъектов ПД

ТЕХНИЧЕСКИЕ МЕРЫ

- ограничение доступа к скомпрометированным системам и базам
- блокировка доступа к источнику инцидента
- смена паролей пользователей и технологических учетных записей
- изоляция затронутых компонентов инфраструктуры
- изменение конфигурации оборудования
- удаление данных для предотвращения повторной утечки

Тактика после инцидента: не допустить повторения

Повторная утечка наказывается оборотным штрафом

Privacy Advocates

1. мониторинг публикаций скомпрометированных ПД и удаление их копий
2. усиление политики ИБ и связанных процедур
3. оценка и обработка рисков ИБ
4. найм дополнительных специалистов и привлечение внешних консультантов по ИБ
5. повышение осведомленности и обучение персонала
6. **добровольное возмещение ущерба и компенсация вреда субъектам ПД**

ТЕХНИЧЕСКИЕ МЕРЫ

- аудит ПО для выявления уязвимостей
- ограничение сетевой доступности сервисов и компонентов
- закупка дополнительных СЗИ: WAF, межсетевые экраны, IDS
- обновление ПО и антивирусных баз
- регулярная проверка доменных учетных записей

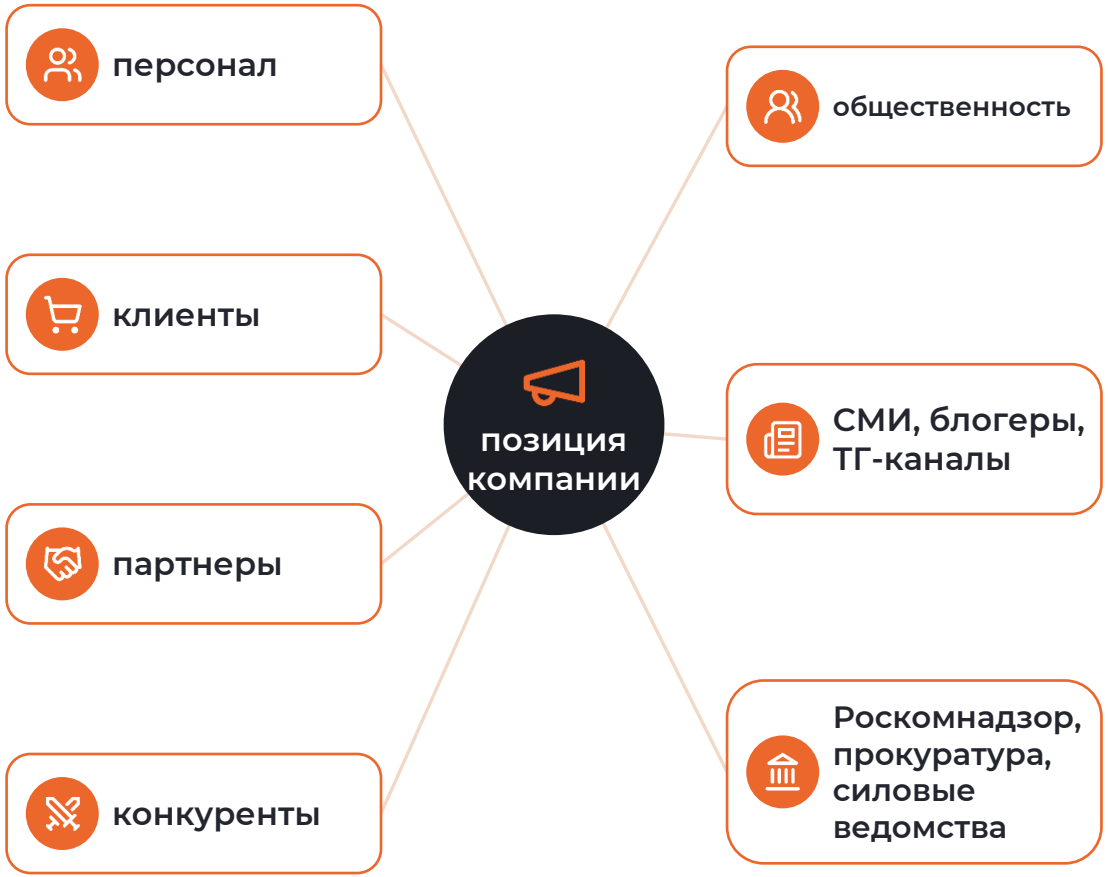
Бонус: по делам, выявленным при контроле, добровольное возмещение вреда и устранение последствий дают право на минимальный штраф по ч.3.4-1 ст.4.1 КоАП

Антикризисный PR: утечка не баг, а фича

С кем говорить и какими техниками управлять повесткой

Privacy Advocates

ЦЕЛЕВАЯ АУДИТОРИЯ



СПИНДОКТОРИНГ



Компенсации пострадавшим: шесть проблем

Почему программы компенсаций редко работают так, как задумано

Privacy Advocates

Объем и характер

любой неунизительный объем и тип компенсации банкротит на масштабе

Высокий забор

слишком высокий порог к компенсации аморален, слишком низкий банкротит

Администрирование

поддержка обращающихся, сложные кейсы и борьба с мошенничеством дорогие и одноразовые

Репутация

в большинстве сценариев программа все равно вредит репутации, а не помогает

Прецедент

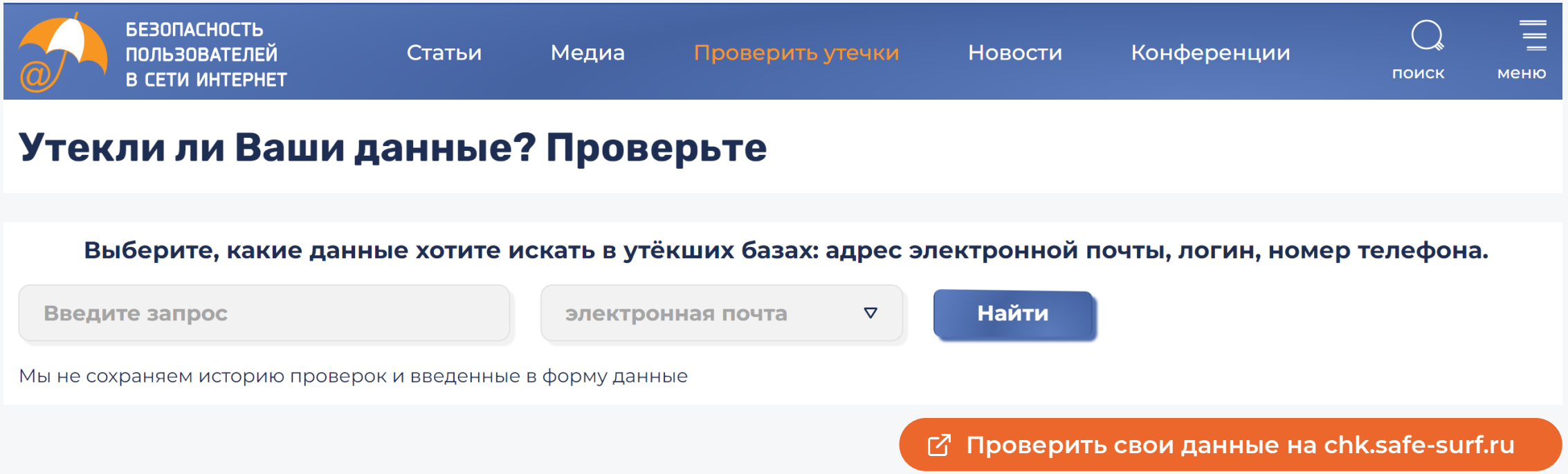
уникальность ситуации порождает нерешенные юридические и налоговые вопросы

Судебные споры

внесудебные компенсации не освобождают от взыскания ущерба в суде

Сервис НКЦКИ помогает субъектам проверить, утекли ли их данные

Проверка по адресу почты, логину или номеру телефона



1. **Узнать о компрометации**
   наличие учетных данных в утекших базах говорит, что они попали к злоумышленникам

2. **Вовремя сменить пароли**
   злоумышленники не всегда сразу используют полученный доступ

3. **Работать над защитой**
   безопасность это постоянный процесс, а не разовая настройка

28.5

План реагирования и плейбук

- План реагирования отвечает на вопрос, кто что делает при инциденте
- Внутри плана: роли, порядок действий и плейбуки
- Реагирование на инцидент идет в семь этапов
- Утвержденный план нужно внедрить и проверить на учениях

План реагирования отвечает на вопрос, кто что делает при инциденте

Incident response plan: крупная утечка - это кризис

Privacy Advocates

План или процедура реагирования - документ, который распределяет роли и действия в случае инцидента. В реагировании бывают задействованы **15 и более функций**, из них собирают слаженную кризисную команду

Кризисная команда

Техника и расследование — 7

- Информационная безопасность
- Инфраструктура
- Команда ИТ продукта
- Инженеры поддержки
- Аналитика данных
- Ситуационный центр
- Служба безопасности

ПД, люди и коммуникации — 5

- DPO
- Клиентский сервис
- PR
- GR
- Кадры

Решения и ресурсы — 4

- Высший менеджмент
- Финансы
- Акционеры и внешние стейкхолдеры
- Внешние консультанты

Внутри плана: роли, порядок действий и плейбуки

Плейбук - настольная инструкция исполнителя

Privacy Advocates

Из чего состоит план

1. фиксация зон ответственности
2. стейкхолдеры от задействованных бизнес-функций
3. общий порядок действий по реагированию
4. плейбуки - инструкции с четким алгоритмом действий для каждого исполнителя

ХОРОШИЙ ПЛЕЙБУК

- только релевантные пункты, а не портянка
- на языке исполнителя
- актуальный
- исчерпывающий

Реагирование на инцидент идет в семь этапов

Кто действует на каждом этапе и что получают на выходе, часть этапов идет параллельно

Privacy Advocates

		ЧТО ДЕЛАЮТ	ЧТО НА ВЫХОДЕ
1	**Выявление**	ответственный получает сведения в единую точку из мониторинга, от сотрудников, публичных источников и третьих лиц и назначает менеджера инцидента	инцидент квалифицирован, анализ и расследование запущены
2	**Анализ и реагирование**	ИБ и ИТ ищут точки компрометации и цепочку событий, закрывают доступы, откатывают фичу, отключают API-метод	последствия сокращены, сведения задокументированы в одном месте
3	**Анализ дампа**	ИБ и ИТ ищут скриншоты, фрагменты и файлы, безопасно загружают и сопоставляют атрибуты с данными компании	статистика совпадений, датировка, характеристики
4	**Подтверждение**	DPO по расследованию, мерам и дампу оценивает наличие ПД, принадлежность компании и нарушение прав субъектов	факт подтвержден или опровергнут, а при нехватке сведений может остаться неподтвержденным
5	**Уведомления**	DPO готовит проекты решений и коммуникаций, менеджмент утверждает в рамках SLA, PR-позиция согласована	решения об уведомлении регулятора, контрагентов, субъектов ПД и о компенсациях
6	**Пост-анализ**	ИБ и DPO определяют организационные меры, технические доработки и изменения процессов подразделений	задачи со сроками и исполнителями
7	**Завершение**	менеджер инцидента и DPO собирают статус принятых и плановых мер, ведут внешние коммуникации, документируют инцидент	этап не оперативный, при недостатках процесс реагирования пересматривают

Открытый вопрос: таймер реагирования запускается при выявлении инцидента (этап 1) или при подтверждении его факта (этап 4)? Разница между ними неочевидна

Утвержденный план нужно внедрить и проверить на учениях

Разработали план с плейбуками - это только начало

Privacy Advocates

шаг 1

Готовность инфраструктуры

- оценка потребности во внешней экспертизе и поддержке
- сбор и хранение логов, внедрение средств защиты
- тикеты и репозитории, доступные всем командам

шаг 2

Подготовка и обучение

- те, кто внедряет, не те, кто исполняет
- настройка систем и инструментов
- шаблоны там, где они нужны

шаг 3

Тестирование плана

- настольные учения (table-top exercise)
- мастер-класс
- симуляция реальной утечки
- на реальном инциденте лучше не стоит

Вывод: план без учений остается документом: слабые места находят на тренировке, а не во время реальной утечки

28.6

Ответственность и практика по утечкам

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OTV-021	До реформы утечки подтверждались, а штрафы были символическими	30 Ответственность
OTV-022	После 30.05.2025 почти каждое расследование подтверждает утечку	30 Ответственность
OTV-002	С 30.05.2025 цена утечки измеряется миллионами и процентами выручки	30 Ответственность
OTV-012	Ст.272.1 УК: шесть составов незаконного оборота ПД	30 Ответственность
OTV-023	Тренды 2025 года по КоАП: предупреждения и мелкие нарушения	30 Ответственность
OTV-026	Минтруд: ошибка подрядчика не спасает оператора от штрафа	30 Ответственность
OTV-025	РЖД: штраф за утечку 17 млн строк отменен за недоказанностью вины	30 Ответственность
OTV-034	DLBI: сервис мониторинга утечек выиграл у Роскомнадзора	30 Ответственность

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
OTV-027	ПКР Аналитика: заявление в полицию не заменяет уголовного дела	30 Ответственность
OTV-028	Комлайн: статус потерпевшего не освобождает от ответственности	30 Ответственность
OTV-029	Орион Телеком: предупреждение устояло только из-за давности	30 Ответственность
OTV-030	Шесть решений по ГК Орион Телеком: виновны, но без штрафа	30 Ответственность
OTV-033	Суды требуют от обеих сторон доказательств мер защиты	30 Ответственность
OTV-018	Ст.272.1 УК: 923 преступления за десять месяцев 2025 года	30 Ответственность
OTV-017	Минцифры: добросовестные ИБ-компании могут работать с утечками	30 Ответственность

ЧАСТЬ

VIII

Надзор, ответственность и практика

Кто проверяет оператора, за что наказывают и как решают суды

29 Взаимодействие с РКН и органами
30 Ответственность за нарушения в области ПД
31 Практика КоАП 2022-2025
32 Резонансные решения 2022-2024

29

Взаимодействие с РКН и органами

Уведомления, проверки, профвизиты и запросы

29.1 Кто контролирует оператора

29.2 Уведомление и реестр операторов

29.3 Проверки, профвизиты и запросы

Раздел на сайте
privacy-advocates.ru/pd/nad

29.1

Кто контролирует оператора

- У оператора несколько контролеров с разным предметом
- От формы запроса органа зависят срок ответа и цена молчания
- Предписание о доступе силовых ведомств исполняют за часы
- Прокуратура проверяет вне ограничений контрольного закона

У оператора несколько контролеров с разным предметом

Карта органов: предмет, инструменты и норма-опора

Материалы РКН
скачать

Privacy Advocates

ОРГАН	ПРЕДМЕТ	ИНСТРУМЕНТЫ	ОПОРА
Роскомнадзор	права субъектов, реестр операторов, требования 152-ФЗ	проверки, визиты, наблюдение, требования, предписания, протоколы	ст.23, 23.1 152-ФЗ, ПП-1046
ФСТЭК России	техническая защита информации	состав мер, сертификация, лицензирование, аттестация, контроль мер в государственных ИСПД	чч.4, 8 ст.19 152-ФЗ, приказы № 21 и № 117
ФСБ России	криптография, ГосСОПКА, дела по чч.1, 2, 6 ст.13.12 КоАП	требования к СКЗИ, лицензирование, предписания о доступе и о копии базы	приказы № 378, 77, 297, 547 и 321, ст.23.46 КоАП
Прокуратура	исполнение законов в целом	запросы и проверки вне 248-ФЗ, представления, требование о проверке Роскомнадзором, иски	ст.6, 21, 22 закона 2202-1
Силовые ведомства	системы со сведениями о защищаемых лицах	доступ по предписанию установленной формы	чч.1.1, 1.2 ст.6 152-ФЗ
Минцифры и Роструд	индикаторы риска; ПД работников по гл.14 ТК	приказ Минцифры № 1187; проверки по ТК, ст.5.27 КоАП	ст.23 248-ФЗ; ст.86-90 ТК

Граница: контроль мер ст.19 Роскомнадзор отсылает к ФСБ и ФСТЭК (письмо от 12.09.2024 № 08-377683), но документарный след мер безопасности нужен все равно

От формы запроса органа зависят срок ответа и цена молчания

Пять форм взаимодействия не взаимозаменяемы: квалификация входящего до подготовки ответа

Privacy Advocates

1. **Контрольное мероприятие по 248-ФЗ**
   проверка, инспекционный визит, рейдовый осмотр: запрос обеспечен ст.19.7 КоАП, воспрепятствование - ч.1 ст.19.4.1
2. **Мероприятие без взаимодействия**
   наблюдение за сайтом и анализ сведений об операторе без уведомления; итог - требование или предостережение
3. **Профилактический визит**
   от обязательного не отказаться, документы истребуются; по заявлению оператора предписаний нет (ч.9 ст.52.2)
4. **Запрос по обращению или о сведениях**
   ч.4 ст.20 152-ФЗ: 10 рабочих дней и не более 5 по мотивированному уведомлению; молчание - ст.19.7 КоАП
5. **Прокурорский запрос**
   закон 2202-1: неисполнение требований прокурора - ст.17.7 КоАП

КВАЛИФИКАЦИЯ ВХОДЯЩЕГО

Четыре шага до ответа

1. орган: от него зависят предмет вопросов и объем раскрытия
2. форма: решение и номер в едином реестре - мероприятие, ссылка на гражданина - рассмотрение обращения
3. режим и срок: считается от даты получения
4. представитель по доверенности и единая точка контакта, лучше ответственный за организацию обработки

Правило: мотивированный отказ лучше молчания: молчание само образует состав, а отказ фиксирует позицию до возбуждения дела

Предписание о доступе силовых ведомств исполняют за часы

Совместный порядок ФСБ, СВР, Минобороны, ФСО и МВД с 11.07.2025 для систем со сведениями о защищаемых лицах

Privacy Advocates

24 часа

назначить ответственного

и сообщить органу с момента получения предписания

3 часа

при незамедлительном доступе

а при гостайне ответственный нужен с допуском

24 часа

сообщить о разглашении

факта предписания и данных должностных лиц, даже неумышленном

ст.19.5.3

КоАП

повышенная санкция за неисполнение такого предписания

Технические причины не основание

скорость обработки, регламентные окна и нерабочее время доступ не откладывают

Без следов прежних записей

должностные лица вносят данные, и журналы не должны раскрывать исходное содержание

Закрытый маршрут

не через общую канцелярию, тикеты и рабочие чаты: в курсе только ответственный и руководитель

ФСБ С 01.04.2026

Две формы предписаний

о доступе к системам с защищаемыми лицами (ст.17 закона о ФСБ, ст.19.5.3 КоАП) и о копии базы данных (ст.15, подписывает руководитель ФСБ, заместитель или начальник территориального органа, специальной санкции нет)

Прокуратура проверяет вне ограничений контрольного закона

Запросы, мониторинг сайтов, представления и иски: чем прокурорский надзор отличается от контроля Роскомнадзора

Privacy Advocates

ЗАКОН 2202-1

Надзор без единого реестра и моратория

прокурор требует документы по предмету проверки (ст.6), обрабатывает ПД по п.2.1 ст.4 и вправе потребовать от Роскомнадзора внеплановой проверки (п.4 ч.1 ст.57 248-ФЗ)

Собственный мониторинг сайтов

Коломна, проверка 20.05.2026: Яндекс Метрика без согласия - ч.1 ст.13.11, нет политики с метрикой - ч.3, штраф 30 тыс. ₽. По ч.1 после отмены 31.08.2026 назначено предупреждение

Детализация систем

запросы требуют имен серверов, СУБД, IP-адресов и схем потоков, а в 2026 году еще и модели угроз и мер по приказу ФСТЭК № 21

Представление

рассмотреть безотлагательно и ответить в месяц (ст.24): нужен ответ, а не согласие, неисполнение - ст.17.7 КоАП

Иск в госсекторе

суд обязал муниципальный орган разработать документы по ст.18.1 и ПП-211 (дело № 2-43/2021)

Учесть: эпизоды прокурорской проверки не объединяют в одно наказание по ч.5 ст.4.4 КоАП. Уплату половины штрафа при прокурорской проверке КС РФ допустил (39-П от 18.07.2024), но на ст.13.11 КоАП эта льгота с 30.05.2025 не распространяется

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
SAJ-003	АС МПД сама находит сайты и ранжирует нарушения	22 Сайт
SAJ-004	Признаки нарушений находят на большинстве проверенных сайтов	22 Сайт

29.2

Уведомление и реестр операторов

- Уведомлять обязан почти каждый оператор, исключений три
- Уведомление заполняют по фактической обработке, а не шаблонно
- Расхождение уведомления с сайтом видно без проверки

Уведомлять обязан почти каждый оператор, исключений три

Круг обязанных лиц после 01.09.2022: где изъятие работает, а где только кажется

Privacy Advocates

Подавать

Уведомление нужно

- любая автоматизация, включая ПК, 1С, сайт и счетчики, снимает бумажное изъятие
- изъятие должно покрывать всю деятельность, иначе в уведомлении отражают и ее
- каждое лицо группы подает свое (письмо Роскомнадзора от 14.08.2026 № 109631-10/77)
- обработчик по поручению, по позиции Роскомнадзора, тоже оператор для уведомления, хотя это спорно
- малый штат и разовые процессы основанием неподачи не служат

vs

Можно не подавать

Изъятие или иная конструкция

- п.7 ч.2 ст.22: ГИС для безопасности государства и общественного порядка
- п.8: обработка исключительно без средств автоматизации
- п.9: случаи законодательства о транспортной безопасности
- гражданин, созывающий собрание собственников, реализует свое право
- иностранное лицо без регистрации в РФ, по позиции управления Роскомнадзора (03.12.2025), подает после создания представительства

Кейс СФО: для специализированного финансового общества без органов и штата Privacy Advocates считает подачу нецелесообразной: обработку ведет управляющая компания. Основание фиксируют письменно, а проект уведомления держат наготове

Уведомление заполняют по фактической обработке, а не шаблонно

Поля уведомления по чч.3 и 3.1 ст.22 152-ФЗ: как заполнять и где ошибаются чаще всего

Privacy Advocates

ПОЛЕ	КАК ЗАПОЛНЯТЬ	ТИПИЧНАЯ ОШИБКА
Цели	по существу: трудовые обязанности одной целью, ДМС отдельной; в графе "иное" формулировка как в политике	одна цель "уставная деятельность" на все процессы
Категории ПД	сами сведения полным перечнем	паспорт и диплом вместо сведений, "и другие"
Правовое основание	отраслевые акты с реквизитами и свои ЛНА	одна ссылка на 152-ФЗ
Действия	только реально совершаемые	весь перечень, включая распространение и обезличивание
Сайт	посетители сайта, cookie и метрика с целью сбора	сайт в уведомлении не отражен
Базы и ТПД	страна и адреса своих мощностей; для ТПД только факт, детали в уведомлении по ст.12	облака спорны: Роскомнадзор устно 14.08.2026 сводит поле к мощностям оператора
Меры, СКЗИ, дата	реально принятый пул мер с последующим дополнением; СКЗИ с документацией; фактическая дата начала	ждут полного пакета мер и не подают



Ловушка: поле в уведомлении об изменении заменяет прежнее содержание записи целиком: вписав только добавленный элемент, оператор стирает остальное

Расхождение уведомления с сайтом видно без проверки

Реестр операторов публичен: уведомление, политику и сайт ведут как единый комплект

Privacy Advocates

3+

ИНДИКАТОР РИСКА, ПРИКАЗ МИНЦИФРЫ № 1187

Три факта несоответствия

сведений уведомлений об обработке и о ТПД политике на сайте дают основание для внепланового мероприятия, и календарным годом этот индикатор не ограничен

КАК ДЕРЖАТЬ КОМПЛЕКТ СИНХРОННЫМ

Единый источник

правка идет из реестра в уведомление, политику и сайт одним событием

Регламент актуализации

изменения до 15-го числа следующего месяца, о прекращении обработки уведомляют в течение 10 рабочих дней; триггеры - новый сервис, смена ответственного, переезд базы

Старые записи

уведомления до 01.09.2022 Роскомнадзор предлагает обновить по форме приказа № 180, жесткого срока нет

Сверка снаружи

прокурор в 2026 году указал, что в реестре не названы посетители сайта и cookie

Учесть: неподача сама основанием проверки не служит, но обнаруживается при любом контакте: по жалобе, запросу или прокурорской проверке. Чаще начинают с информационного запроса, и ответ на него нужен в течение 10 рабочих дней

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
BAZ-026	Уведомление РКН об обработке ПД	03 Обзор комплаенса
SAJ-018	Об обработке и о ТПД уведомляют раздельно и заранее	22 Сайт
TPD-024	Содержание уведомления о намерении	20 ТПД

29.3

Проверки, профвизиты и запросы

- Главный канал надзора - профилактический визит
- Категория риска задает только плановую нагрузку
- Ответ на запрос по жалобе становится доказательством
- У каждого акта органа своя сила, срок и санкция

Главный канал надзора - профилактический визит

Первое полугодие 2026 года и устройство обязательного визита после ПП-1286

Privacy Advocates

728

профилактических визитов

за первое полугодие 2026 года

1

внеплановая проверка

за тот же период, а в 2024 году плановых не было

89

предписаний

выдано по итогам визитов

504

нарушения

выявлено, из них 490 по ст.13.11 КоАП

Обязательный

Инициатива органа

- уведомление за 24 часа, отказаться нельзя
- срок до 10 рабочих дней (ПП-1286)
- документы истребуются, осмотр возможен дистанционно
- неустраненное к концу визита - предписание

По заявлению

Инициатива оператора

- малый бизнес, социально ориентированные НКО и учреждения
- разъяснения носят рекомендательный характер
- предписаний не выдают (ч.9 ст.52.2)

АКТ ВИЗИТА

Три исхода

1. нарушений нет
2. устранены до конца визита
3. не устранены - предписание

Категория риска задает только плановую нагрузку

Риск-модель ПП-1046 в редакции ПП-1286: группа тяжести, группа вероятности и что из них следует

Privacy Advocates

КАТЕГОРИЯ РИСКА НА ПЕРЕСЕЧЕНИИ ГРУПП

тяжесть	группа вероятности: история санкций 1	2	3	4
А	высокий	значительный	значительный	средний
Б	высокий	значительный	средний	умеренный
В	значительный	значительный	средний	умеренный
Г	средний	средний	умеренный	низкий

КРИТЕРИИ ГРУПП ТЯЖЕСТИ

А: спецкатегории и биометрия, более 100 тыс. субъектов, лишнее согласие, иностранные сервисы сбора, передача обезличенных

Б: дети, более 10 тыс. субъектов, зарубежные базы, обезличивание без передачи

В: родственники, 1-10 тыс. субъектов, ТПД в адекватные страны

Г: менее 1 тыс. субъектов, общедоступные источники

Вероятность - это история санкций

группы 1-3 по актам реагирования за 2 года и постановлениям за 3 года, группа 4 - их нет

Плановая нагрузка

высокий риск: проверка раз в 2 года или визит в год; значительный, средний, умеренный: визит не чаще раза в 3, 5 и 6 лет (ПП-1511)

Комплаенс категорию не понижает

безупречный оператор всегда в группе 4, а лишнее согласие и обезличивание с передачей поднимают тяжесть до А

Индикаторы вне категории

четыре порога приказа Минцифры № 1187 дают внеплановое мероприятие при любой категории

Ответ на запрос по жалобе становится доказательством

Лестница эскалации по обращению субъекта и вилка из трех исходов ответа регулятору

Privacy Advocates

1 **Жалоба регулятору**
субъект жалуется на оператора

2 **Запрос**
10 рабочих дней и не более 5 сверху

3 **Требование**
исполнить или пояснить за 10 рабочих дней

4 **Дело**
по заявлению гражданина

5 **Обжалование**
субъект бывает потерпевшим

6 **Иск**
компенсация и обязание

честный ответ

Приложено неполное письмо заявителю

оно само доказывает состав ч.4 ст.13.11 КоАП (дело № 05-1546/419/2024, оператору назначено предупреждение)

уклончивый ответ

Версия расходится с гражданином

десять расхождений за год дают индикатор риска и внеплановое мероприятие

молчание

Запрос проигнорирован

самостоятельный состав ст.19.7 КоАП и потеря возможности объясниться до дела

Выход один: ответить заявителю полно с первого раза, а перед ответом регулятору проверить свое письмо и при неполноте направить заявителю дополнение

У каждого акта органа своя сила, срок и санкция

Предостережение, требование, предписание и представление прокурора: что исполнять, что оспаривать и когда

Privacy Advocates

АКТ	СИЛА	СРОК РЕАКЦИИ	ЗА НЕИСПОЛНЕНИЕ
Предостережение	обязанности не создает	возражение за 10 рабочих дней (п.20 ПП-1046)	состава нет
Требование уточнить или уничтожить	обязательно	исполнить или пояснить за 10 рабочих дней	чч.5, 5.1 ст.13.11
Требование прекратить обработку	обязательно	срок называет само требование	своей части нет, ст.19.5 спорна
Предписание	обязательно	исполнить в срок, жалоба за 10 рабочих дней	ч.1 ст.19.5 КоАП
Представление прокурора	ответ, не согласие	месяц (ст.24 закона 2202-1)	ст.17.7 КоАП

Сверка до начала мероприятия | основание из закрытого перечня ч.1 ст.57 248-ФЗ | согласование с прокуратурой | номер в едином реестре | уведомление за 24 часа | удостоверения и QR-код | пороки по ст.91 - отмена результатов

Иной режим: расследование по утечке идет по КоАП без моратория и согласования с прокуратурой, а истребованные сведения дают за 3 дня (ст.26.10, 28.7 КоАП)

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
RSK-005	Регулятор уже мыслит рисками	26 Прайваси-риски
INC-012	По утечке Роскомнадзор сначала запрашивает документы	28 Инциденты
KOA-003	Дела начинаются с жалоб, а отказы в возбуждении часты	31 Практика КоАП

С регулятором выигрывает тот, кто готов заранее

Выводы раздела

Privacy Advocates

01

Сначала квалификация

кто обратился и в какой форме: от этого зависят срок, обязательность ответа и цена молчания

02

Уведомление как зеркало реестра

уведомлять обязан почти каждый, а уведомление, политику и сайт сверяют снаружи без проверки

03

Визит вместо проверки

обязательный профилактический визит стал главным каналом надзора, и к нему готовятся как к проверке

04

Категория - не щит

риск-модель отражает свойства обработки и историю санкций, а индикаторы и жалобы работают вне нее

05

Ответ - это доказательство

письмо регулятору с приложениями собирает состав, его проверяют до отправки, а спор о предписании решают в первые 10 дней

30

Ответственность за нарушения в области ПД

Составы, санкции и практика 2025-2026

30.1 Пакет законов 2024 и ландшафт

30.2 Административная ответственность

30.3 Уголовная ответственность

30.4 Практика 2025-2026

Раздел на сайте
privacy-advocates.ru/pd/otv

30.1

Пакет законов 2024 и ландшафт

- Законы 2024-2025 годов резко ужесточили ответственность за ПД
- С 30.05.2025 цена утечки измеряется миллионами и процентами выручки
- Ландшафт юридической ответственности за ПД

Законы 2024-2025 годов резко ужесточили ответственность за ПД

Три закона об усилении административной и уголовной ответственности

Privacy Advocates

420-ФЗ от 30.11.2024

КоАП: утечки и биометрия

- оборотные штрафы за повторные утечки, до 500 млн ₽
- шкала штрафов по числу субъектов и идентификаторов
- составы о неуведомлении Роскомнадзора
- новая ст.13.11.3 о биометрии
- действует с 30.05.2025

421-ФЗ от 30.11.2024

УК: ст.272.1

- незаконные использование, передача, сбор и хранение компьютерной информации с ПД
- создание ресурсов для незаконного оборота ПД
- до 10 лет лишения свободы
- действует с 11.12.2024

104-ФЗ от 23.05.2025

КоАП: защита информации

- ужесточение ст.13.12 КоАП
- до 100 тыс. ₽ для ЮЛ за несертифицированные СЗИ и нарушение требований о защите
- давность по ст.13.12 увеличена до 1 года

С 30.05.2025 цена утечки измеряется миллионами и процентами выручки

Главное в 420-ФЗ: шкала по масштабу, повторность и биометрия

Privacy Advocates

до 15 млн ₽

Разовая утечка

ч.12-14 ст.13.11 по масштабу: от 3 млн ₽ уже при 1-10 тыс. субъектов

1-3% выручки

Повторная утечка

ч.15 и ч.18: не менее 20 или 25 и не более 500 млн ₽

до 20 млн ₽

Утечка биометрии

ч.17, а утечка специальных категорий до 15 млн ₽ по ч.16

до 3 млн ₽

Неуведомление об утечке

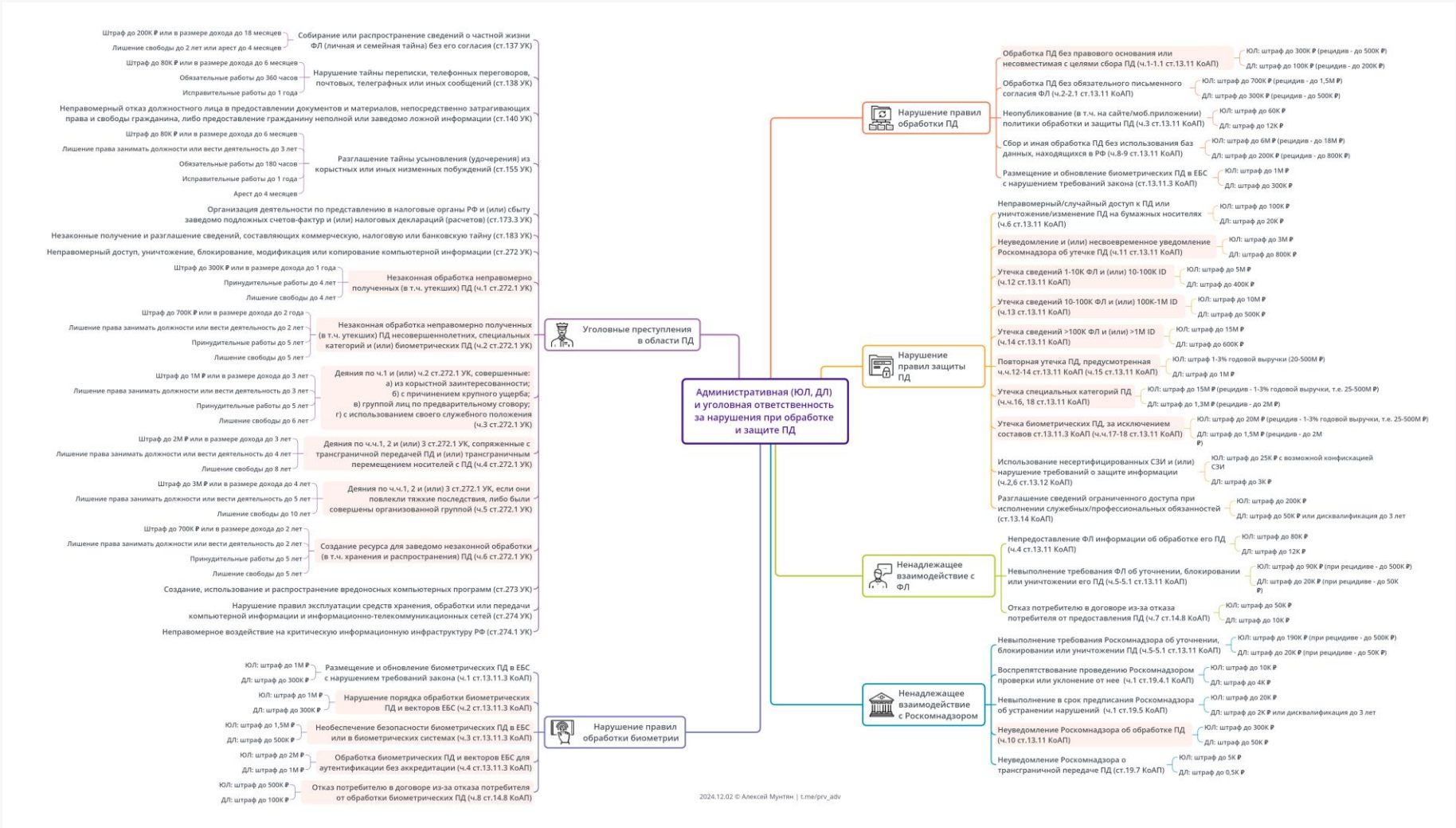
ч.11, а неуведомление об обработке до 300 тыс. ₽ по ч.10

- штрафы по ч.1-1.1 и ч.2-2.1 ст.13.11 выросли до 300 тыс. и 700 тыс. ₽, при повторности до 500 тыс. и 1,5 млн ₽
- новые ст.13.11.3 о биометрии в ЕБС и биометрических системах и ч.8 ст.14.8 об отказе потребителю, не согласному на биометрию
- ИП в ч.1.1 и 8-18 ст.13.11 отвечают как юридические лица
- оборотный штраф по ч.15 и ч.18 снижается до 1/10 минимума при трех условиях ч.3.4-2 ст.4.1

Ландшафт юридической ответственности за ПД

Административная и уголовная ответственность за нарушения при обработке и защите ПД

Privacy Advocates



Карта в полном размере

на Яндекс Диске

30.2

Административная ответственность

- Штраф за утечку растет с масштабом, категорией и повторностью
- Неуведомление и биометрия наказываются отдельными составами
- Новые составы КоАП: кто отвечает и что отягчает
- Новые составы оставили открытыми пять вопросов

Штраф за утечку растет с масштабом, категорией и повторностью

Санкции ст.13.11 КоАП за обработку без оснований и утечки, ₽

Privacy Advocates

ЧАСТЬ СТ.13.11	НАРУШЕНИЕ	ЮРИДИЧЕСКОЕ ЛИЦО	ДОЛЖНОСТНОЕ ЛИЦО
ч.1 и 1.1	обработка без основания или несовместимая с целями сбора	150-300 тыс., повторно 300-500 тыс.	50-100 тыс., повторно 100-200 тыс.
ч.2 и 2.1	без обязательного письменного согласия	300-700 тыс., повторно 1-1,5 млн	100-300 тыс., повторно 300-500 тыс.
ч.11	неуведомление Роскомнадзора об утечке	1-3 млн	400-800 тыс.
ч.12	утечка: 1-10 тыс. субъектов или 10-100 тыс. ID	3-5 млн	200-400 тыс.
ч.13	утечка: 10-100 тыс. субъектов или 0,1-1 млн ID	5-10 млн	300-500 тыс.
ч.14	утечка: более 100 тыс. субъектов или 1 млн ID	10-15 млн	400-600 тыс.
ч.15	повторная утечка по ч.12-14	**1-3% выручки, 20-500 млн**	800 тыс.-1,2 млн
ч.16	утечка специальных категорий ПД	10-15 млн	1-1,3 млн
ч.17	утечка биометрических ПД	15-20 млн	1,3-1,5 млн
ч.18	повторная утечка спецкатегорий или биометрии	**1-3% выручки, 25-500 млн**	1,5-2 млн

Неуведомление и биометрия наказываются отдельными составами

Санкции за неуведомление и обработку биометрических ПД, ₽

Privacy Advocates

НОРМА КОАП	НАРУШЕНИЕ	ЮРИДИЧЕСКОЕ ЛИЦО	ДОЛЖНОСТНОЕ ЛИЦО
ч.10 ст.13.11	неуведомление или несвоевременное уведомление Роскомнадзора об обработке ПД	100-300 тыс.	30-50 тыс.
ст.19.7	непредставление сведений в Роскомнадзор; применение к неуведомлению о ТПД спорно	3-5 тыс.	300-500
ч.1 ст.13.11.3	размещение и обновление биометрических ПД в ЕБС с нарушением закона	500 тыс.-1 млн	100-300 тыс.
ч.2 ст.13.11.3	нарушение порядка обработки биометрических ПД и векторов ЕБС	500 тыс.-1 млн	100-300 тыс.
ч.3 ст.13.11.3	необеспечение безопасности биометрических ПД в ЕБС или в биометрических системах	1-1,5 млн	300-500 тыс.
ч.4 ст.13.11.3	обработка биометрии и векторов ЕБС для аутентификации без аккредитации	1-2 млн	500 тыс.-1 млн
ч.8 ст.14.8	отказ потребителю в договоре из-за отказа от идентификации или аутентификации по биометрии	200-500 тыс.	50-100 тыс.

Новые составы КоАП: кто отвечает и что отягчает

Особенности ч.10-18 ст.13.11, действующих с 30.05.2025

Privacy Advocates

Субъекты

- должностное лицо - ДЛ госоргана, муниципального органа или НКО
- юридическое лицо - иной оператор
- ИП в ч.1.1 и 8-18 приравнены к юридическим лицам

Отягчающие для ч.15 и ч.18

- продолжение нарушения вопреки требованию прекратить его (п.1 ч.1 ст.4.3)
- нарушитель подвергнут наказанию по ч.1-11 ст.13.11, ст.13.6 или 13.12 на момент нарушения

Обработчик и уведомления

- за утечку у обработчика отвечает оператор, поручивший обработку
- ч.10 формально не охватывает уведомления о ТПД, изменении сведений и прекращении обработки, но иногда к ним применяется

Новые составы оставили открытыми пять вопросов

Проблематика ч.10-18 ст.13.11 и порядка производства

Privacy Advocates

1. **Обратная сила**

   дискуссионно применение новых составов к нарушениям до 30.05.2025 с учетом ст.1.7 КоАП

2. **Идентификатор**

   как выделять ID среди иных сведений, определять уникальность, считать повторы в одной БД и квалифицировать ID вне ИСПД; не будет ли привязка к ID дестимулировать переход со сквозных идентификаторов на локальные

3. **Неуведомление об утечке**

   ч.11 касается только Роскомнадзора, но не ФСБ, и не отвечает, длящееся это нарушение или продолжаемое

4. **Расследование**

   по ч.1-2.1 и 12-18 при экспертизе и долгих процессуальных действиях обязательно административное расследование (ст.28.7), которое устанавливает и вину

5. **Подсудность**

   с 30.05.2025 дела по ст.13.11 рассматривали арбитражные суды, с 01.01.2026 они вернулись в суды общей юрисдикции (508-ФЗ от 28.12.2025), а принятые арбитражем до этой даты остались у него

ЛОВУШКА ПЕРЕХОДА

Давность

протокол, направленный в арбитражный суд в конце 2025 года, после передачи по подсудности поступил в районный суд за пределами годичного срока, и производство прекращено за давностью

Общие смягчающие нормы КоАП работают и для дел о ПД

Четыре ступени: от освобождения до минимального штрафа

Privacy Advocates

01

Освобождение от ответственности

при малозначительности правонарушения, ст.2.9

02

Предупреждение

за впервые совершенное нарушение без вреда, угрозы вреда и ущерба, ч.1 ст.4.1.1 и ч.2 ст.3.4. В 2026 году мировые судьи дали его в 8 из 83 актов

03

Половина штрафа

при исключительных обстоятельствах, связанных с характером и последствиями нарушения и материальным положением ЮЛ, ч.3.2-3.3 ст.4.1

04

Минимальный штраф

по делам, выявленным при контроле, если предотвращены последствия, возмещен ущерб или устранен вред, ч.3.4-1 ст.4.1 и пп.5-6 ч.1 ст.4.2

ВАЖНО

- широкое применение ст.2.9 и ч.3.2-3.3 ст.4.1 к ч.15 и ч.18 ст.13.11 маловероятно
- оплата в течение 20 дней не дает скидки 50% (ч.1.3-3 ст.32.2)
- организация и ее должностное лицо обычно отвечают параллельно, исключения - ч.4-5 ст.2.1, в том числе оборотные штрафы по ч.15 и ч.18
- см. п.21 постановления Пленума ВС РФ от 24.03.2005 № 5

Оборотный штраф снижается до 1/10 минимума при трех условиях

Особое смягчение по ч.3.4-2 ст.4.1 КоАП для ч.15 и ч.18 ст.13.11

Privacy Advocates

Штраф снижается до **одной десятой минимального размера**, но не менее 15 и не более 50 млн ₽, если одновременно выполнены все условия:

1

Расходы на ИБ

не менее 0,1% годовой выручки в каждом из трех предшествующих лет на мероприятия, проведенные лицензиатами ФСТЭК (ТЗКИ) или ФСБ (СКЗИ) либо самим оператором с лицензией

2

Подтверждение защиты

документально подтвержденное соблюдение требований к защите ПД в ИСПД в течение 12 месяцев до выявления нарушения

3

Нет отягчающих

отсутствуют отягчающие обстоятельства по примечанию 5 к ст.13.11: продолжение нарушения или действующее наказание по смежным составам

Открытые вопросы: засчитают ли сервисы и СЗИ не от лицензиатов и в какой форме подтверждать соблюдение требований к защите, практика пока не ответила

Смягчение по утечке: что работает, а что нет

Общие институты КоАП и специальное снижение оборотного штрафа

Privacy Advocates

Малозначительность ст.2.9 КоАП	по утечкам работает редко и только по совокупности обстоятельств
Замена на предупреждение ст.4.1.1, ч.2 ст.3.4	впервые, при госконтроле, нет вреда и угрозы. По ч.13 практика расходится, апелляция 14.08.2026 сочла замену незаконной
Штраф ниже низшего предела чч.3.2-3.3 ст.4.1	исключительные обстоятельства, санкция от 100 тыс. ₽, не менее половины минимума
Минимальный штраф ч.3.4-1 ст.4.1	дело выявлено при контроле, вред предотвращен или добровольно возмещен
Снижение оборотного штрафа ч.3.4-2 ст.4.1	до 1/10 минимума, в пределах 15-50 млн ₽: ИБ не менее 0,1% выручки 3 года силами лицензиатов, подтверждение защиты за год, нет отягчающих

ОБЫЧНО НЕ РАБОТАЕТ

- ✕ нас взломали без доказательств мер: дело РЖД (10.06.2026) помогает, только если меры показаны
- ✕ утекшее не ПД: даже имя с телефоном относится к лицу
- ✕ виноват подрядчик: перед субъектом отвечает оператор
- ✕ данные устарели: статус ПД держится до уничтожения
- ✕ работник осужден по ст.272.1 УК: организацию не освобождает
- ✕ быстрая оплата: скидка 50% к ст.13.11 не применяется

Четыре опоры защиты

1. обстоятельства инцидента: масштаб, категории, экспозиция
2. статус и поведение: впервые, признание, устранение
3. меры до и во время: документы, ИБ, оценка вреда
4. действия после: уведомления, оповещение, компенсации

С 23.05.2025 нарушения защиты информации стоят дороже

104-ФЗ ужесточил ст.13.12 КоАП и продлил давность

Privacy Advocates

НОРМА	НАРУШЕНИЕ	ГРАЖДАНИН	ДОЛЖНОСТНОЕ ЛИЦО	ЮРИДИЧЕСКОЕ ЛИЦО
ч.2 ст.13.12	использование несертифицированных информационных систем, баз данных и СЗИ, если сертификация обязательна	5-10 тыс.	10-50 тыс.	50-100 тыс.
ч.6 ст.13.12	нарушение требований о защите информации, кроме государственной тайны	5-10 тыс.	10-50 тыс.	50-100 тыс.

Также: срок давности по ст.13.12 увеличен до 1 года со дня совершения правонарушения, а наказание по ст.13.12 отягчает ответственность за повторную утечку

30.3

Уголовная ответственность

- Ст.272.1 УК: шесть составов незаконного оборота ПД
- Ст.272.1 УК: особенности и вопросы применения
- Ст.272.1 УК и ст.13.11 КоАП частично совпадают
- Предлагается разграничить УК и КоАП по законности цели обработки

Ст.272.1 УК: шесть составов незаконного оборота ПД

Незаконные использование, передача, сбор и хранение компьютерной информации с ПД, полученной неправомерно

Privacy Advocates

ЧАСТЬ	СОСТАВ	МАКСИМАЛЬНОЕ НАКАЗАНИЕ
ч.1	незаконные использование, передача, сбор, хранение компьютерной информации с ПД, полученной неправомерным доступом или иным вмешательством	штраф до 300 тыс. ₽ или дохода за 1 год, принудительные работы или лишение свободы до 4 лет
ч.2	то же с ПД несовершеннолетних, специальных категорий или биометрическими	штраф до 700 тыс. ₽ или дохода за 2 года, принудительные работы или лишение свободы до 5 лет
ч.3	ч.1 или 2 из корыстной заинтересованности, с крупным ущербом, группой по сговору или с использованием служебного положения	штраф до 1 млн ₽ или дохода за 3 года, принудительные работы до 5 лет, лишение свободы до 6 лет
ч.4	ч.1-3, сопряженные с трансграничной передачей ПД или перемещением носителей	лишение свободы до 8 лет со штрафом до 2 млн ₽ и лишением права до 4 лет
ч.5	ч.1-4 с тяжкими последствиями или организованной группой	**лишение свободы до 10 лет**
ч.6	создание или обеспечение работы ресурса, заведомо предназначенного для незаконного хранения или распространения ПД	штраф до 700 тыс. ₽, принудительные работы или лишение свободы до 5 лет

Ст.272.1 УК: особенности и вопросы применения

Что важно знать о новой статье

Privacy Advocates

Способ получения

ч.1-5 требуют, чтобы ПД были получены неправомерным доступом или иным вмешательством в средства обработки либо иным незаконным способом

Личные нужды

статья не применяется к обработке ПД физлицами исключительно для личных и семейных нужд

Трансграничность

наряду с передачей ПД учитывается перемещение машиночитаемого носителя с ПД через границу

Тяжкие последствия

собственного определения статья не содержит

ПРОГНОЗ ПРАКТИКИ

- при смягчающих обстоятельствах суды скорее выберут штраф и лишение права занимать должность, а лишение свободы оставят для масштабных и резонансных дел
- п."е" ч.1 ст.61 УК о зависимости позволяет суду снизить категорию преступления (ст.15 УК)
- в уголовном деле можно заявить гражданский иск о компенсации морального и имущественного вреда (ст.151, 1099 ГК, ст.44 УПК)
- ориентир - постановление Пленума ВС РФ от 15.12.2022 № 37 о компьютерных преступлениях

Ст.272.1 УК и ст.13.11 КоАП частично совпадают

Верховный Суд предупреждал о конкуренции норм еще на стадии законопроекта

Privacy Advocates

> В диспозиции части 1 проектной статьи 272.1 УК РФ отсутствуют криминообразующие признаки, позволяющие отграничить соответствующее преступление от противоправных действий, предусмотренных статьей 13.11 КоАП РФ...

Отзыв Верховного Суда РФ на законопроект от 11.01.2023 № 4-ВС-79/23, заместитель Председателя ВС РФ В.А. Давыдов

РАЗЛИЧИЯ

1. в КоАП ответственным лицом назван оператор, в УК нет
2. КоАП говорит об информации с ПД, УК о компьютерной информации с ПД

РИСК

одно и то же деяние может быть квалифицировано и как правонарушение, и как преступление, в т.ч. в зависимости от субъективной оценки его общественной опасности

Предлагается разграничить УК и КоАП по законности цели обработки

Возможное решение: незаконность цели как криминообразующий признак

Privacy Advocates

Фокус на субъективной стороне: уголовно наказуемой должна быть обработка ПД для цели, **прямо запрещенной законом**. Противоправная обработка ПД ради изначально законной цели, например исследовательской, не должна квалифицироваться как преступление

ОПОРА

Пленум ВС РФ № 58 от 22.12.2015

характер общественной опасности определяется уголовным законом и зависит от направленности деяния на охраняемые им ценности и от причиненного вреда

Уголовная ответственность

обработка ради запрещенной цели: продажа баз, мошенничество, преследование

Административная ответственность

нарушение правил обработки при законной цели деятельности

Граница УК и КоАП при утечке

Два трека ответственности идут параллельно и не заменяют друг друга

Privacy Advocates

Оператор как организация

ст.13.11 КоАП

- отвечает за непринятие мер, повлекшее утечку
- осуждение работника не освобождает и не доказывает отсутствие вины
- уголовное дело может влиять на административную квалификацию

Работник, инсайдер, внешний нарушитель

ст.272.1, 272, 137, 183 УК

- отвечает лично, только при умысле
- организация к уголовной ответственности не привлекается
- топ-менеджеров оператора пока судят по ст.274 УК (дело Сирена-трэвел)

ЗОНА КОНКУРЕНЦИИ

- ВС в отзыве на проект (11.01.2023): в ч.1 нет криминообразующих признаков, это ведет к конкуренции со ст.13.11 КоАП
- Диспозиция ч.1 широка: формально покрывает почти любую неправомерную обработку оцифрованных ПД
- Экспертный подход: решает цель - противоправная обработка ради законной цели (например, исследовательской) не должна вести к уголовному преследованию
- Спорно: руководитель или ответственный как соучастник при обработке базы из сомнительного источника

Не принимать данные из сомнительных источников
хранения с осознанием незаконности происхождения уже достаточно

Разводить треки
содействие расследованию и одновременно собственная защита по КоАП

Сохранять доказательства
атаки, работы защиты и реагирования до любых изменений

Минцифры: добросовестные ИБ-компании могут работать с утечками

Позиция о применении ст.272.1 УК

Privacy Advocates

Кому грозит ответственность

- тем, кто незаконно использует, передает, собирает и хранит ПД, доступ к которым получен неправомерно
- тем, кто создает и обеспечивает работу ресурсов, где такая информация хранится и распространяется

Неправомерный доступ

- незаконное воздействие на серверы, компьютеры и сети для нарушения обработки и хранения ПД
- например взлом, незаконное проникновение и кража

ИБ-специалисты

- для расследования утечек им приходится иметь дело с незаконно распространяемыми данными
- закон допускает такую обработку, например для защиты жизни, здоровья и иных интересов граждан

Ст.272.1 УК: 923 преступления за десять месяцев 2025 года

Кого привлекают и за что

Privacy Advocates

923

преступления по ст.272.1

зарегистрировано за 10 месяцев 2025 года, раньше многие квалифицировали по ст.137, 272, 274 УК

Кого привлекают

работников салонов связи, сотрудников правоохранительных органов, МФЦ и налоговых служб, курьеров банков, медиков

DPO

случаев привлечения DPO не отмечено; должность важна только для специальных составов

Боты и брокеры

под ответственность попадают владельцы ботов для поиска данных, например Userbox, и серые дата-брокеры

Типичные деяния

слив данных конкретному лицу, схемы с сим-картами, продажа сканов паспортов, фото с экранов компьютеров

Уголовные дела за утечки: инсайдеры и доступ к КИИ

Сводная таблица дел по ст.274.1 и 272.1 УК, 2024-2025

Privacy Advocates

СТАТЬЯ УК	ЧТО СДЕЛАНО	КТО	ИТОГ
ч.5 ст.274.1	атака на систему бронирования авиабилетов, завладение ПД пассажиров	два вице-президента разработчика системы	дело возбуждено в 2024 году
ч.5 ст.274.1	установил ПО удаленного доступа к медсистеме "ПроМед" для ритуального агентства	системный администратор станции скорой помощи, Астрахань	**5 лет условно**
п."г" ч.3 ст.272.1	передал посторонним ПД заслуженного артиста и еще одной абонентки	сотрудник салона связи, Кировск	дела возбуждены
ст.272.1	36 запросов за три месяца и продажа данных абонентов за криптовалюту	сотрудник салона связи, Новосибирск	дело по материалам ФСБ
п."г" ч.3 ст.272.1	передавал знакомым сведения из единого реестра недвижимости	начальник отдела филиала публично-правовой компании, Карелия	дело возбуждено СК
ч.2 ст.272.1	сфотографировала экран с диагнозом пациентки и разослала в мессенджере	уборщица районной больницы, Свердловская область	**штраф 10 тыс. ₽**

Тренд: в этой выборке большинство дел возбуждено против сотрудников с доступом к данным, а не против внешних хакеров

Уголовные дела за утечки: продажа данных и ресурсы для их оборота

Сводная таблица дел по ст.272.1 УК, 2025

Privacy Advocates

СТАТЬЯ УК	ЧТО СДЕЛАНО	КТО	ИТОГ
ч.3 ст.272.1	сообщила ФИО и адрес абонента третьему лицу по телефону и в мессенджере	специалист телеком-компании, Хакасия	дело возбуждено МВД
ч.3 ст.272.1	продал мошенникам данные более 27 тыс. человек	руководитель колл-центра МФЦ и медучреждений, Череповец	**заключен под стражу**
ст.272.1	сервис продажи доступа к утекшим базам: подписка порой дороже 1 млн ₽ в месяц, изъято более 25 ТБ	организатор и его техподдержка	**под стражей**
ч.3 и 5 ст.272.1	регистрация более 1500 сим-карт по купленным сканам паспортов	трое партнеров оператора связи, Красноярский край	дело возбуждено
ч.2 ст.183; п."г" ч.3 ст.272.1	сбор налоговой тайны и передача ПД третьим лицам	налоговый инспектор (ст.183) и сотрудница казначейства (соучастие и ст.272.1), Калуга	дело возбуждено СК
ч.5 и 6 ст.272.1	Telegram-бот "Юзер Бокс" (Userbox) распространял ПД из утечек	создатель и администратор бота, Санкт-Петербург	**обвинение предъявлено**

Пример: дело Userbox показывает, что ч.6 ст.272.1 применяют к создателям ресурсов, а не только к тем, кто передает конкретные записи

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
INC-002	Закон знает три дефиниции утечки, и они не совпадают	28 Инциденты

30.4

Практика 2025-2026

- До реформы утечки подтверждались, а штрафы были символическими
- После 30.05.2025 почти каждое расследование подтверждает утечку
- Тренды 2025 года по КоАП: предупреждения и мелкие нарушения
- Практика 2026 года по утечкам: первые решения по новым составам

До реформы утечки подтверждались, а штрафы были символическими

Статистика Роскомнадзора до реформы ответственности

Privacy Advocates

135

утечек в 2024

710 млн записей

168

утечек в 2023

300 млн записей

140

утечек в 2022

600 млн записей

2023 ГОД

4,6 млн ₽ штрафов

39 внеплановых проверок, в 37 утечки подтвердились, 122 протокола, по 87 из них назначены штрафы по ч.1 и ч.2 ст.13.11

- вместо штрафа нередко назначали предупреждение (ст.4.1.1) или освобождали от ответственности за малозначительностью (ст.2.9)
- практика шла по пути объективного вменения: оператора привлекали за утечку без установления вины (ст.2.1)

После 30.05.2025 почти каждое расследование подтверждает утечку

Первые итоги применения новых составов, данные 2025 года

Privacy Advocates

16

административных расследований

по фактам неправомерной передачи ПД, повлекшей нарушение прав субъектов

15

утечек подтверждено

территориальными органами Роскомнадзора

ч.1, 12, 13

ст.13.11 КоАП

составы, по которым составлены протоколы

Новое: протоколы составлены и по новым составам ч.12 и ч.13 с санкциями от 3 и от 5 млн ₽ для юридических лиц

Тренды 2025 года по КоАП: предупреждения и мелкие нарушения

Распределение дел и особенности привлечения к ответственности

Privacy Advocates

РАСПРЕДЕЛЕНИЕ ПО СОСТАВАМ СТ.13.11

СОСТАВЫ	ДОЛЯ
ч.1-1.1: незаконная обработка и небольшие утечки	**почти 2/3**
ч.3-6: политика, права субъектов, требования РКН, ручная обработка	**около 1/5**
ч.2-2.1: нет обязательного письменного согласия	**единицы %**
ч.8-9: нелокализация баз с ПД	**единицы %**

Предупреждения

больше половины дел 2025 года закончились предупреждением, а в 2026 году у мировых судей 8 из 83 актов

Инициаторы

около трех четвертей дел начинает Роскомнадзор, остальные прокуратура

Кого привлекали

банки, телеком, госучреждения, школы, больницы, цифровые сервисы, УК, ТСЖ и СНТ, физлица

Новые спецсоставы

в 2025 году крупных штрафов не было, в 2026 арбитраж дал 400 тыс. ₽ по ч.14 (ЮКИДС) и предупреждение по ч.13

Практика 2026 года по утечкам: первые решения по новым составам

Ч.1 и чч.12-16 ст.13.11 КоАП: суммы, исходы и спор о границе составов

Privacy Advocates

ДЕЛО	СОСТАВ	ИТОГ	ЧТО ВАЖНО
ЮКИДС, А40-351064/2025	ч.14	**400 тыс. ₽**	микропредприятию штраф снижен по ст.4.1.2 до ставки должностного лица, замены предупреждением нет, 9 ААС 03.06.2026 оставил
Орион Телеком, А19-25808/2025	ч.13	предупреждение	впервые и без вреда, 4 ААС 14.08.2026 оставил
МК НАКФФ, 05-1258/252/2026	ч.16	**5 млн ₽**	утечка данных пациентов: штраф снижен для среднего предприятия, сумма в копии обезличена, по имеющимся сведениям 5 млн ₽ при минимуме 10 млн ₽, в силе с 15.09.2026
МГЭУ, 05-669/2026	ч.1	**150 тыс. ₽**	утечку данных 2486 абитуриентов квалифицировали по ч.1, хотя субъектов больше тысячи
Ростелеком, А56-82945/2025	чч.1, 12	не привлечен	кассация 02.10.2026: оператор отвечает за подрядчика, но срок давности истек

Спор: граница ч.1 и ч.12 не устоялась: утечки ниже порогов идут по ч.1, а прежние утечки через подрядчика суды то выводят из ч.1, то возвращают. Объем затронутых данных фиксируют сразу после инцидента

РЖД: штраф за утечку 17 млн строк отменен за недоказанностью вины

Апелляция и кассация потребовали от Роскомнадзора доказать вину оператора

Privacy Advocates

ДЕВЯТЫЙ ААС 16.02.2026, АС МО 10.06.2026, № А40-263206/2025

Штраф 150 тыс. ₽ отменен

Роскомнадзор нашел в Telegram-каналах базу сотрудников РЖД более 17 млн строк: ФИО, должности, email. Первая инстанция оштрафовала по ч.1 ст.13.11. РЖД сослались на целенаправленную атаку, по ч.1 ст.272.1 УК возбуждено уголовное дело

КЛЮЧЕВЫЕ ВЫВОДЫ

- сам факт утечки не равен вине компании, административная ответственность наступает только при вине (ч.2 ст.2.1 КоАП)
- Роскомнадзор обязан доказать, какие меры компания могла, но не приняла
- если воля компании направлена на защиту, а вред нанесли преступники, вины оператора в административном смысле нет
- вывод о вине преждевременен, пока не завершено уголовное дело о взломе; геополитический фон снижает степень вины

Важно: это вывод по конкретному делу: в делах Комлайн, ПКР Аналитика и Орион суды признали вину операторов, несмотря на кибератаки и статус потерпевшего

Минтруд: ошибка подрядчика не спасает оператора от штрафа

ВС РФ оставил в силе штраф за утечку данных сотрудников

ВС РФ, 21.01.2026, № 5-АД25-119-К2

Штраф 100 тыс. ₽ по ч.1 ст.13.11

В ноябре 2023 года в сеть утекли данные сотрудников министерства и их родственников. Минтруд ссылался на взлом инфраструктуры подрядчика, который не обеспечил защиту

КЛЮЧЕВЫЕ ВЫВОДЫ

- статус оператора обязывает принимать организационные и технические меры защиты, передача обработки подрядчику не снимает ответственности
- министерство не уведомило Роскомнадзор само и подтвердило утечку только после запроса регулятора, это расценено как бездействие
- нет доказательств внутреннего контроля и аудита соответствия обработки требованиям ст.18.1, 19 и 22.1 152-ФЗ

ПКР Аналитика: заявление в полицию не заменяет уголовного дела

Первая инстанция применила ч.13 ст.13.11, но заменила штраф предупреждением

Privacy Advocates

АС СПБ И ЛО, 26.02.2026, № А56-4733/2026

Предупреждение по ч.13 ст.13.11

В августе 2025 года после кибератаки в Telegram попала база интернет-ресурса: 70 тыс. представителей и сотрудников юрлиц, ФИО, должность, служебные email и телефон. Компания вовремя направила первичное и вторичное уведомления

КЛЮЧЕВЫЕ ВЫВОДЫ

- суд отказал приостановить дело из-за проверки в полиции: выписка КУСП не равна постановлению о возбуждении уголовного дела
- вина признана, но за первое нарушение штраф заменен предупреждением по ст.4.1.1 КоАП даже при 70 тыс. субъектов
- суды первой инстанции продолжают объективное вменение и требуют от оператора доказать все возможные меры защиты

Комлайн: статус потерпевшего не освобождает от ответственности

Отчет о расследовании, представленный самим оператором, лег в основу решения

Privacy Advocates

АС КЕМЕРОВСКОЙ ОБЛАСТИ 28.04.2026, СЕДЬМОЙ ААС 27.08.2026, № А27-23786/2025

Предупреждение по ч.12 ст.13.11

В июне 2025 года группировка BO_Team_UA скомпрометировала данные 4 225 абонентов: ФИО, паспорта, адреса, телефоны. Отчет BI.ZONE, заказанный самим оператором, показал активную учетку уволенного в 2022 году сотрудника, пароли с 2019 года и уязвимое ПО

КЛЮЧЕВЫЕ ВЫВОДЫ

- уголовное дело по ст.272.1 против хакеров не освобождает оператора, составы разграничивают ответственность злоумышленника и оператора
- статус объекта КИИ 3 категории не дает права на утечку
- затягивание процесса и позднее ходатайство об экспертизе суд расценил как злоупотребление правом
- санкция 3-5 млн ₽ заменена предупреждением: МСП и первое нарушение

Коммуникация: компания сначала называла инцидент DDoS-атакой и отрицала утечку, а признала ее только после публикации базы

Орион Телеком: предупреждение устояло только из-за давности

Апелляция сочла предупреждение за утечку 36 544 субъектов назначенным вопреки закону

Privacy Advocates

АС ИРКУТСКОЙ ОБЛАСТИ 12.05.2026, ЧЕТВЕРТЫЙ ААС 14.08.2026, № А19-25808/2025

Предупреждение по ч.13 ст.13.11

База опубликована в Telegram 29.07.2025. Защита настаивала, что проникновение 30.05.2025 не позволяет применить ч.13. Компания - потерпевший по уголовному делу по ст.272, 273 и 272.1 УК

КЛЮЧЕВЫЕ ВЫВОДЫ

- состав материальный: нарушение окончено в момент неправомерной передачи, то есть публикации базы
- ст.272.1 УК наказывает злоумышленника, ст.13.11 КоАП - неисполнение оператором обязанностей по защите, составы разграничены
- вопрос вины правовой, поэтому в экспертизе о степени вины суд отказал
- апелляция: утечка паспортных данных, адресов и телефонов - существенное нарушение прав, условий ч.2 ст.3.4 для предупреждения нет

Итог: наказание не ужесточили только из-за истечения годичной давности, отсчитанной от публикации базы. Практика по предупреждениям при объемных утечках разошлась

Шесть решений по ГК Орион Телеком: виновны, но без штрафа

АС Красноярского края, 15.05.2026: закрытые заседания и предупреждения

Privacy Advocates

1. **Закрытые заседания**
   допустимы, когда в деле детали ИТ-инфраструктуры и результаты внутренних аудитов ИБ

2. **Вина признана**
   по всем делам компании привлечены за необеспечение защиты ПД, наказание "иное" - предупреждение

3. **Подмена понятий**
   пресс-релиз о "невиновности в распространении" подменил предмет: судили не за распространение, а за необеспечение безопасности

ПРИВЛЕЧЕНЫ К ОТВЕТСТВЕННОСТИ

6 компаний, 8 решений

- ООО "Орион Телеком", Красноярск: А33-29341/2025, А33-29658/2025, А33-29660/2025
- ООО "Орион Телеком", Красноярский край
- ООО "КрисТелеком"
- ООО "45 КА"
- ранее: ООО "Комлайн" и ООО "Орион Телеком", Иркутск

Отзовик: суд не увидел ПД в отзыве со скрытым ФИО

Суд поддержал отказ Роскомнадзора возбудить дело против площадки отзывов

Privacy Advocates

АС Г. МОСКВЫ, 07.11.2025, № А40-236948/2025

Отказ ИП в требованиях

ИП оспорил отказ Управления Роскомнадзора по ЦФО возбудить дело против администратора Otzovik.com, где был отзыв с его данными и порочащими сведениями

КЛЮЧЕВЫЕ ВЫВОДЫ

- ФИО частично скрыты звездочками, это исключает идентификацию
- адрес в отзыве относится к складу в Москве, а заявитель зарегистрирован в Туле
- заявитель не доказал связь с компанией из отзыва
- площадка - информационный посредник и не отвечает за чужие публикации без знания о незаконности (постановление КС РФ от 09.07.2013 № 18-П)

Передача ПД работника бухгалтеру и арендодателю не требует согласия

Обработка для исполнения трудового договора и обязанностей работодателя

САВЕЛОВСКИЙ РАЙОННЫЙ СУД, 16.07.2025, № 02-2324/2025

Согласие не требовалось

В трудовом споре работница заявила, что работодатель незаконно передал ее ПД компании, ведущей бухгалтерский и налоговый учет, и арендодателю офиса для оформления пропуска

КЛЮЧЕВЫЕ ВЫВОДЫ

- работодатель вправе обрабатывать ПД работника без отдельного письменного согласия, если это нужно для исполнения трудового договора и обязанностей работодателя
- опора - ч.1 ст.86 ТК РФ и п.5 ч.1 ст.6 152-ФЗ

Практика: передача обработчику по поручению или для пропускного режима остается в рамках договорного основания

Суды требуют от обеих сторон доказательств мер защиты

Запросы судов по делам ГК Орион Телеком

Privacy Advocates

A74-10378/2025

Что запросил суд

- Роскомнадзор описывает меры, которые общество должно было, но не приняло
- ответчик описывает и документально подтверждает принятые меры защиты

A33-29369/2025

Что запросил суд

- Роскомнадзор оценивает доводы о системах защиты, обосновывает дату доступа к ИСПД и момент окончания правонарушения
- ответчик доказывает принятие всех необходимых превентивных мер

Вывод: доказательства мер защиты собирают до инцидента: после утечки их уже не создать

DLBI: сервис мониторинга утечек выиграл у Роскомнадзора

Поиск по хешам без хранения ПД в открытом виде не признан обработкой ПД

Privacy Advocates

АС Г. МОСКВЫ 10.12.2025, ДЕВЯТЫЙ ААС 14.04.2026, АС МО 08.07.2026, № А40-201075/2025

В привлечении отказано в трех инстанциях

Роскомнадзор по данным своей системы АС МПД считал DLBI посредником, дающим доступ к нелегальным базам без оснований (ч.1 ст.13.11). DLBI разделил обработку данных посетителей сайта и поисковый алгоритм, который работает с хешами, и предоставляет проверку через партнеров

КЛЮЧЕВЫЕ ВЫВОДЫ

- сервис обрабатывает не ПД, а данные, в которых ищутся признаки ПД пользователей
- Роскомнадзор не доказал, что анализируемые сведения являются охраняемыми законом ПД
- деятельность DLBI соответствует мировой практике и направлена на предупреждение утечек

Значение: Роскомнадзор проиграл, потому что не доказал, что анализируемые сведения являются ПД; модель сервиса суд отдельно не оценивал

Что дальше: возможна дифференциация штрафов по масштабу бизнеса

Законодатель заявил о мониторинге применения оборотных штрафов

Privacy Advocates

> ...по итогам анализа, возможно, появится более дифференцированная шкала в отношении различных юрлиц...

Андрей Клишас, глава Комитета Совета Федерации по конституционному законодательству и государственному строительству, 26.11.2024

ЧТО ОБСУЖДАЛОСЬ

1. разные наказания для крупных и небольших банков
2. дискуссия с отраслевыми лоббистами продолжается

ЗА ЧЕМ СЛЕДИТЬ

1. практику по ч.15 и ч.18 ст.13.11 КоАП
2. применение ч.3.4-2 ст.4.1 КоАП о снижении оборотного штрафа

Ответственность за ПД: чем дальше, тем строже

Ключевые выводы раздела

Privacy Advocates

01

Утечка стоит миллионы

с 30.05.2025 штраф зависит от масштаба, категории данных и повторности, а повторная утечка стоит до 3% выручки

02

Вина снова в фокусе

по РЖД суды потребовали доказать вину оператора, но в большинстве дел о кибератаках вину признают

03

Предупреждение - не победа

это наказание: год лицо считается подвергнутым ему, что отягчает ответственность по ч.15 и ч.18 (прим.5 к ст.13.11)

04

Доказательства мер заранее

расходы на ИБ, подтверждение соблюдения требований и расследование готовят до инцидента

05

Уголовный риск у инсайдеров

ст.272.1 УК чаще всего применяют к сотрудникам с легальным доступом к данным

31

Практика КоАП 2022-2025

Составы ст.13.11 и 13.12 КоАП в цифрах

Раздел на сайте
privacy-advocates.ru/pd/koa

Дела 2022-2025 годов учтены по решению последней инстанции

Как собрана выборка: 725 дел по ст.13.11 и 7 дел по ст.13.12 КоАП за 01.2022-05.2025

Privacy Advocates

732

ВЫБОРКА PRIVACY ADVOCATES

01.2022-05.2025

публично доступные тексты судебных актов, прямо или косвенно связанных с ПД и ст.13.11, 13.12 КоАП

Что не учтено

обжалование отказов в возбуждении дела, административные иски по КАС РФ и гражданские споры

Последняя инстанция

если дело прошло несколько инстанций, в статистику вошел результат рассмотрения в последней

Связки органов

прокуратура и ФСБ, прокуратура и Роскомнадзор, МВД и Роскомнадзор, МВД и прокуратура: первый участник обычно ведет доследственную проверку или фиксирует нарушение, второй возбуждает и расследует дело

Факт не равен штрафу

штраф заменяют предупреждением (ст.4.1.1 КоАП) или освобождают от ответственности за малозначительностью (ст.2.9 КоАП)

Обновление: практика по тем же частям за 06.2025-10.2026 и статистика 2026 года - на двух последних слайдах подраздела, санкции после 420-ФЗ и тренды 2025 года - в разделе 30

Две трети дел по ст.13.11 - обработка без основания

Составы по частям за 01.2022-05.2025: три четверти дел по ч.1-1.1 начинает Роскомнадзор

Privacy Advocates

ЧАСТЬ И НАРУШЕНИЕ	ДЕЛ	МОСКВА	ЮЛ И ИП / ДЛ / ФЛ	РКН / ПРОКУРАТУРА	ПРЕДУПРЕЖДЕНИЙ	ОПРАВДАТЕЛЬНЫХ
ч.1-1.1 ст.13.11: обработка без основания	**475**	230	305 / 106 / 47	359 / 116	51	64
ч.2-2.1: без письменного согласия	**94**	47	70 / 19 / 5	68 / 26	2	17
ч.3: политика не опубликована	11	3	2 / 8 / 5	4 / 7	-	2
ч.4: нет ответа субъекту об обработке	27	14	15 / 9 / 3	22 / 5	6	4
ч.5-5.1: требование субъекта не исполнено	42	19	21 / 9 / 12	42 / -	6	8
ч.6: доступ к ПД на бумажных носителях	11	4	5 / 6 / -	9 / 2	-	1
ч.8-9: сбор ПД без баз в России	**65**	63	57 / 7 / 1	65 / -	-	6
ч.2 ст.13.12: несертифицированные СЗИ	2	-	1 / 1 / -	ФСБ 2	-	1
ч.6 ст.13.12: требования о защите	5	1	2 / 5 / -	ФСБ 3 / 2	-	2

Дела начинаются с жалоб, а отказы в возбуждении часты

Что решало исход дел по ч.1-5.1 ст.13.11 КоАП в 2022-2025 годах

Privacy Advocates

ч.1-1.1, 475 дел

частый повод - жалобы граждан на компании и органы власти. Утечки в Telegram и на сайтах суды считают достаточным основанием, в отличие от жалоб без доказательств. Проверки по распоряжениям высокого уровня, например зампреда Правительства, идут в приоритете и заканчиваются протоколами. **Из 106 наказанных ДЛ 9 - DPO**

ч.2-2.1, 94 дела

по этому составу квалифицируют и утечки ПД работников. Роскомнадзор регулярно отказывает в возбуждении дела по п.1 или 2 ч.1 ст.24.5 КоАП: нет события или состава. **Из 19 наказанных ДЛ 2 - DPO**

ч.3, 11 дел

большинство дел начинается с жалобы, около 40% заканчиваются отказом в возбуждении. Кредитный потребительский кооператив оштрафован: в опубликованной политике назван другой сайт

ч.4, 27 дел

жалобы на отсутствие ответа, в 40-50% случаев отказ в возбуждении по формальным основаниям: нет доказательств обращения или дан формальный ответ. Работодатель оштрафован, когда не ответил бывшему работнику со ссылкой на локальные акты, с которыми тот ознакомлен под подпись

ч.5-5.1, 42 дела

жалобы на игнорирование требований уточнить или удалить ПД. Требование гражданина суды часто считают формально неподтвержденным, но несвоевременный или уклончивый ответ оператора квалифицируют как нарушение

Практика: исход дел по ч.3-5.1 решают доказательства обращения субъекта и ответа оператора

Дела о нелокализации касаются в основном иностранцев, ст.13.12 редка

Ч.6 и 8-9 ст.13.11 и ч.2, 6 ст.13.12 КоАП в практике 2022-2025 годов

Privacy Advocates

ч.6 ст.13.11, 11 дел

Бумажные носители

- утеря или ненадлежащее хранение документов с ПД
- среди нарушителей много ФГБУ, ГБУ, школ и больниц
- нет контроля доступа к личным делам и журналам регистрации
- нарушение вскрывается после жалобы, утечки или внутренней проверки

ч.8-9 ст.13.11, 65 дел

Базы за пределами России

- чаще всего сбор ПД через интернет без базы в РФ
- большинство фигурантов - иностранные ЮЛ, часть привлечена повторно
- дело возбуждают после дистанционного контроля Роскомнадзора или отказа выполнить его предписание

СТ.13.12 КОАП, 7 ДЕЛ

Только по материалам ФСБ и прокуратуры

- ч.2, 2 дела: несертифицированные СЗИ, ФСТЭК среди инициаторов и участников нет
- ч.6, 5 дел: все связаны с утечками, доступ к файлам без авторизации зафиксирован надзорным актом
- предупреждений, дисквалификаций и конфискаций нет, DPO не наказывались
- санкции ст.13.12 после 104-ФЗ - в разделе 30

Пример ч.6 ст.13.12: в мероприятии "Кибер-щит" УФСБ сканером ripgrep проверило публичные ссылки Google Drive и нашло архив Ведомость_дети.zip с ФИО и адресами учеников центра допобразования

Практика 2025-2026: больше предупреждений и регионов

Судебные акты по ст.13.11 КоАП с 2022 года по частям до и после 30.05.2025, данные на 21.10.2026

Privacy Advocates

ЧАСТЬ	ДО 30.05.2025	ПОСЛЕ	ШТРАФ	ПРЕДУПРЕЖДЕНИЕ	ПРЕКРАЩЕНО	ИНОЕ
ч.1-1.1	503	296	144	82	21	49
ч.2-2.1	47	20	9	4	5	2
ч.3	11	13	7	6	-	-
ч.4	28	24	12	2	4	6
ч.5-5.1	44	9	5	2	-	2
ч.6	11	3	-	1	-	2
ч.8-9	70	37	31	-	-	6
ч.10	-	13	6	5	1	1
ч.12-18	-	13	3	6	1	3

ЧТО ИЗМЕНИЛОСЬ ПОСЛЕ 30.05.2025

- доля предупреждений по ч.1-1.1 выросла **с 8% до 28%** актов
- регионы дают **70%** актов по ч.1-1.1 против 47% раньше
- по ч.10 о неуведомлении больше половины дел возбуждает прокуратура
- по утечкам ч.12-18 в 6 актах из 13 предупреждение, дела Комлайн, Орион Телеком и ПКР Аналитика - в разделе 30
- в 2026 году картина развернулась, см. следующий слайд

Важно: здесь считается каждый акт инстанции, а выборка 2022-2025 - дело по последней инстанции, поэтому сравнивают доли, а не числа

В 2026 году предупреждение снова стало редкостью

После возврата дел по ст.13.11 в суды общей юрисдикции с 01.01.2026: акты 2026 года на 21.10.2026

Privacy Advocates

8 из 83

мировые судьи

актов с заменой штрафа предупреждением, из них 5 по прокурорским делам о муниципальных учреждениях

41 из 72

арбитражные суды

замена штрафа предупреждением в первой инстанции по делам, принятым до 01.01.2026

150 000 ₽

медиана у мировых

штраф по ч.1 ст.13.11 у мировых судей

75 000 ₽

медиана в арбитраже

штраф по ч.1 ст.13.11 в арбитражных судах

Арбитражное окно закрылось

с 30.05.2025 по 31.12.2025 дела по ст.13.11 рассматривали арбитражные суды, и предупреждение было обычным исходом

Утечек в судах мало

по обзору практики за январь-август 2026 года актов об утечках по ч.12-17 всего 12

Тренды 2025 года

общие доли предупреждений и составов за 2025 год - в разделе 30 "Ответственность"

ОРИЕНТИР ДЛЯ НОВЫХ ДЕЛ

Минимальный штраф, а не предупреждение

у мировых судей реалистичная цель - минимальный штраф либо штраф ниже низшего предела там, где он допустим

32

Резонансные решения 2022-2024

Десять решений, которые изменили практику

32.1 Работодатель и ПД работников

32.2 Почта, распространение, локализация, согласие

Раздел на сайте
privacy-advocates.ru/pd/kej

32.1

Работодатель и ПД работников

- ПД работника передают без согласия по трудовому договору
- Проверка конфликта интересов по СПАРК - законный интерес
- Работодатель поручает обработку ПД работника без его согласия
- Работодатель вправе сообщать о дисциплинарных взысканиях

ПД работника передают без согласия по трудовому договору

АС Московского округа по спору Аэрофлота и Роскомнадзора о предписании, 30.05.2022

Privacy Advocates

A40-163911/2021

Аэрофлот выиграл в трех инстанциях

компания оспорила пункты предписания Управления Роскомнадзора по ЦФО. АС г. Москвы удовлетворил требования, Девятый ААС и АС Московского округа оставили решение в силе

ВЫВОДЫ СУДА

- прекращать обработку ПД бывших работников через пять лет после увольнения не обязательно
- документы, в том числе архивные, можно хранить и в бумажном, и в электронном виде
- понятия "документ, переведенный в статус архивного" закон не знает: сроки приказа Росархива от 20.12.2019 № 236 применяются, потому что документ есть в перечне
- согласие на передачу ПД работника (ст.88 ТК) должно отвечать ч.4 ст.9 152-ФЗ, только если это специальные категории, биометрия или ТПД в неадекватные страны
- без согласия работодатель передает ПД работника в случаях пп.2-11 ч.1 ст.6 152-ФЗ, и п.5 о договоре распространяется на трудовые отношения

Позиция Роскомнадзора: п.5 ч.1 ст.6 применим только к гражданско-правовым договорам, а основания обработки в трудовых отношениях задает гл.14 ТК

Проверка конфликта интересов по СПАРК - законный интерес

Центральный районный суд г. Кемерово, 30.09.2022, № 12-532/2022: ПД работника из открытых источников

Privacy Advocates

1

Антикоррупционные ЛНА

ВТБ по ч.2 ст.11 и ч.1-2 ст.13.3 закона о противодействии коррупции ввел положение об урегулировании конфликта интересов, работники с ним ознакомлены

2

Внутренняя проверка

комиссия по пп.7.3 и 7.4 положения проверила работников по СПАРК и официальному сайту ФНС

3

Находка

один работник оказался директором и совладельцем другой организации с долей 33%

4

Жалобы

Управление Роскомнадзора по Кемеровской области - Кузбассу семь раз отказало работнику в проверке банка

5

Суд

отказ Роскомнадзора оставлен в силе, состава ч.2 ст.13.11 КоАП нет, актов вышестоящих инстанций в базе нет

Вывод суда: истребование работодателем сведений о работнике из открытых источников для проверки конфликта интересов - обработка в законном интересе оператора по п.7 ч.1 ст.6 152-ФЗ, если не нарушены права и свободы работника

Работодатель поручает обработку ПД работника без его согласия

Пресненский районный суд г. Москвы, 30.01.2024, № 2-907/2024: собственный законный интерес

Privacy Advocates

2-907

ПРЕСНЕНСКИЙ РАЙОННЫЙ СУД

В иске работнику отказано

работник СК Энмув Рус оспорил право работодателя передавать его ПД третьим лицам и поручать им обработку без согласия. Акты вышестоящих инстанций не найдены

01

Договор и закон

обработка в трудовых отношениях ведется для исполнения договора и закона и не ставится под условие согласия, иначе договор нельзя заключить и исполнить

02

Собственный интерес

работодатель вправе передавать ПД и поручать их обработку третьим лицам в своем законном интересе, если права работников не нарушены

03

Электронный архив

документы хранят и в электронном виде, ПД уволенных сохраняются в течение сроков хранения, в том числе в информационных системах

04

Копии - не ПД

частичная утрата кадровых документов не нарушает прав работника: копии - носители ПД, и их утрата не означает утраты ПД

Работодатель вправе сообщать о дисциплинарных взысканиях

Постановление КС РФ от 21.07.2023 № 44-П: распространение, опровержение и пределы ответственности

Privacy Advocates

КС проверял п.1 ст.152 ГК по делу работника, которого наказали приказом и сообщили об этом коллегам, а потом суд приказ отменил

1

Приказ и стенды

работник наказан, сведения о проступке размещены на стендах внутри организации

2

Суд отменил приказ

проступок не доказан, и сведения не соответствуют действительности с момента издания приказа

3

Опровержение

добросовестный работодатель сообщает о незаконности приказа, согласовав это с работником

4

Судебная защита

если работодатель уклоняется от опровержения, работник требует его в суде

ПРАВО РАБОТОДАТЕЛЯ

определять, нужно ли распространять сведения о взыскании и насколько подробно описывать нарушение, если содержание соответствует цели и **очевидно с ней связано**

БЕЗ КОМПЕНСАЦИИ

если сведения распространены **добросовестно** до признания приказа незаконным, убытки и моральный вред с работодателя не взыскиваются

Согласие работника по строгому образцу требовать нельзя

Первый КСОЮ, 18.06.2024, № 88-19257/2024: отказ в ДМС и дотации на питание незаконен

Privacy Advocates

НЕСТЛЕ РОССИЯ

Иск работника удовлетворен частично

работник дал согласие на обработку ПД по своей форме, а не по типовой форме работодателя, и лишился ДМС и дотации на питание. Первый КСОЮ оставил решение в силе

Можно ли лишить льгот за согласие не по форме работодателя?

Нет, требовать согласие по строгому образцу и лишать за отказ дополнительных льгот нельзя

В какой форме дается согласие?

В любой форме, позволяющей подтвердить факт его получения (ч.1 ст.9 152-ФЗ)

Что еще повлияло на исход?

Работодатель не доказал, что объяснил работнику, чего не хватает в его согласии и почему без этого передача ПД третьему лицу не имеет основания

Можно ли признать недействительным локальный акт?

Трудовое право такого понятия не знает: права, нарушенные локальным актом, защищаются только в индивидуальном трудовом споре

Практика: тот же подход - в определении Третьего КСОЮ от 18.12.2023 № 88-25965/2023

Фото работника в рекламе вакансий требует письменного согласия

Второй КСОЮ, 04.07.2023, № 88-13675/2023: участие в съемке еще не согласие на имиджевое использование

Privacy Advocates

ПОЗИЦИЯ СУДА ПО СПОРУ С ГК НОРНИКЕЛЬ

Согласие - сделка

письменная, устная или конклюдентная (п.46 постановления Пленума ВС РФ от 23.06.2015 № 25, ст.153, 158 ГК), устное охватывает цели, очевидные из обстановки (п.47)

Съемка не равна согласию

фото с корпоративной съемки для поощрения работников нельзя ставить на сайт вакансий, а зарплата за рабочий день не плата за позирование

ТК и биометрия

абз.3 ст.88 ТК запрещает сообщать ПД работника в коммерческих целях без письменного согласия, а фото, по которому можно идентифицировать человека, суд счел биометрическими ПД

ЧТО ОХВАТЫВАЕТ ПИСЬМЕННОЕ СОГЛАСИЕ

1. распространение биометрических ПД работника
2. использование в коммерческих целях
3. использование работодателем и компаниями группы
4. использование в период работы и после увольнения

Итог: кассация оставила в силе 80 000 ₽ компенсации с ПАО ГМК "Норильский никель", а в части запрета использовать фото направила дело на новое рассмотрение

32.2

Почта, распространение, локализация, согласие

- ПД по закону раскрывают без согласия на распространение
- E-mail - ПД, но сайт не обязан проверять его владельца
- Бремя доказать локализацию лежит на операторе
- Согласие на обработку нельзя навязать условиями договора

ПД по закону раскрывают без согласия на распространение

ВС РФ, 21.07.2023, № 305-ЭС23-12160 по спору Роскомнадзора и СК Арсеналъ

Privacy Advocates

Распространение

Согласие по ст.10.1 - частный случай согласия

- распространять ПД можно и по другим пунктам ч.1 ст.6 152-ФЗ
- ПД руководителей и участников страховщик раскрывает по пп.2 и 11 ч.1 ст.6 во исполнение пп.2 п.6 ст.6 закона об организации страхового дела
- ни ст.10.1, ни другие нормы не требуют согласия на обработку во исполнение обязанностей и требований закона о раскрытии

Электронная почта

Адрес сам по себе не ПД

- как и по номеру телефона, по одному адресу без других идентификаторов нельзя определить конкретное лицо
- довод Роскомнадзора о неизменности и уникальности адреса отклонен
- адрес не абсолютно неизменен: после удаления ящика его может зарегистрировать новый пользователь, как номер нового абонента

Итог: ВС РФ отказал в передаче жалобы. Как суды то применяют, то отвергают критерий уникальности e-mail, показано в разделе 05 "Определение ПД"

E-mail - ПД, но сайт не обязан проверять его владельца

ВС РФ, 29.12.2023, № 310-ЭС23-26429 по спору УФАС по Смоленской области и 2ГИС о рекламе

Privacy Advocates

УФАС считало адрес электронной почты не относящимся к ПД и сомневалось, что согласие на рекламу можно получить по адресу без проверки его владельца

E-mail - ПД

это подтверждают п.1 ст.3 152-ФЗ, постановление Правительства от 13.09.2019 № 1197 и письмо Минцифры от 17.03.2022 № П25-5623

Действия под учеткой

совершенное под учетной записью считается сделанным пользователем, пока он не сообщил о несанкционированном доступе

Без верификации

владелец сайта по общему правилу не обязан и не может подтверждать, что адрес принадлежит конкретному лицу

Форма согласия

обязательная письменная форма согласия на рекламную рассылку на e-mail не нужна

Итог: суды поддержали 2ГИС, ВС РФ отказал УФАС в передаче жалобы

Бремя доказать локализацию лежит на операторе

Дела Ookla о сервисе Speedtest: 1 млн ₽ по ч.8 и 6 млн ₽ по ч.9 ст.13.11 КоАП

Privacy Advocates

7 млн ₽

ШТРАФЫ OOKLA

Обе санкции устояли в кассации

- **1 млн ₽ по ч.8**: мировой судья 12.07.2022, Таганский районный суд, Второй КСОЮ 26.12.2022
- **6 млн ₽ по ч.9**, повторно: мировой судья 16.10.2023, Таганский районный суд, Второй КСОЮ 14.03.2025

Нацеленность не нужна

нет русского интерфейса, политики на русском, расчетов в рублях и доставки, но регистрация россиян не ограничена, значит локализация применима

248-ФЗ не защищает

требования 248-ФЗ и постановления Правительства от 10.03.2022 № 336 к лицам за пределами РФ не применяются

Что локализуют

данные о сетевой активности, идентификаторы устройства и cookie, полученные при мониторинге поведения

E-mail как ID

если для регистрации нужен только адрес, который нельзя использовать повторно, это уникальный идентификатор и ПД

Бремя доказывания

по делу о 6 млн ₽ нахождение баз в том или ином государстве доказыванию не подлежит: локализацию доказывает оператор

Вывод: иностранному ресурсу нужны меры ограничения доступа россиян: указание гражданства до доступа, блокировка российских IP-адресов

Согласие на обработку нельзя навязать условиями договора

Кировский районный суд г. Уфы: решения от 04.12.2023 № 2-12745/2023 и 11.12.2023 № 2-12744/2023

Privacy Advocates

ПУБЛИЧНЫЙ РЕЖИМ

Договор не восполняет закон

режим обработки ПД установлен публично. Где закон связывает с договором согласие на соразмерную обработку, банк не вправе регулировать это условиями договора: суд расценил это как **приватизацию сферы позитивного правового регулирования**, что недопустимо

МЕХАНИЗМ СОГЛАСИЯ ПО ПОЗИЦИИ СУДА

1. отношения согласия инициирует субъект, а не оператор: нельзя получить то, что не было дано
2. устанавливают факт дачи согласия, а не пассивного невозражения против навязанного
3. свобода выразить несогласие не форма дачи согласия
4. свобода отозвать согласие не означает свободы его выражения
5. отзыв показывает отношение субъекта к обработке, но положительной формой согласия не является

Итог: навязанные условия о согласиях признаны ничтожными, иски к МТС-Банку и Промсвязьбанку удовлетворены частично, с МТС-Банка взыскано 10 тыс. ₽ морального вреда. Акты вышестоящих инстанций не найдены

Согласие не панацея: суды ищут иные основания и реальную волю

Пять выводов из десяти резонансных решений 2022-2024 годов

Privacy Advocates

1. **Работодатель не заложник согласия**
   ПД работника передают и поручают по договору, закону и законному интересу: Аэрофлот, ВТБ, СК Энмув Рус
2. **Согласие - воля, а не бланк**
   его не требуют по образцу и не навязывают договором: Нестле, банки в Уфе
3. **Коммерция - письменно**
   имиджевое использование фото работника - только с письменным согласием: Норникель
4. **E-mail зависит от контекста**
   сам по себе не ПД (Арсеналъ), но ПД в сервисе 2ГИС и при регистрации в Ookla
5. **Локализацию доказывает оператор**
   иностранный сервис, открытый россиянам, держит базы в России: Ookla, штрафы 1 и 6 млн ₽ устояли в кассации

Девиз: в прайваси комплаенсе у вас не бывает проблем, у вас бывают приключения

ЧАСТЬ

IX

Отраслевые разборы

Как общие правила работают в адвокатуре, банкротстве и фармаконадзоре

33 ПД в адвокатской практике

34 ПД в процедуре банкротства

35 ПД в фармаконадзоре

33

ПД в адвокатской практике

Как адвокату не поменяться ролями с подзащитным

33.1 Адвокат как оператор

33.2 Где хранится и чем пользуемся

33.3 Цена вопроса и первые шаги

Раздел на сайте
privacy-advocates.ru/pd/adv

33.1

Адвокат как оператор

- Адвокат становится оператором с первого звонка доверителя
- Один том дела - несколько режимов конфиденциальности
- Разъяснение ФПА 2025 года сняло спор адвокатуры о статусе оператора

Адвокат становится оператором с первого звонка доверителя

Режим ПД и режим адвокатской тайны не отменяют друг друга, а накладываются

Privacy Advocates

ЧТО АДВОКАТ ПОЛУЧАЕТ С ПЕРВОГО ЗВОНКА

ФИО | телефон | паспорт | адрес | **здоровье** | **судимость** | **личная жизнь**

Часто это **специальные категории ПД**. Поверх них - адвокатская тайна (ст.8 63-ФЗ) и чужие охраняемые тайны, которые адвокат получает вместе с делом

ТИПИЧНАЯ ОШИБКА

Тайна не заменяет статус оператора

без уведомления, политики и кадрового контура комплаенс не закрыт

ДВА РЕЖИМА

Соблюдать нужно оба

- по 152-ФЗ адвокат - оператор, и его обязанности сохраняются
- ст.8 63-ФЗ: тайна покрывает все сведения, связанные с юридической помощью, включая ПД доверителя
- тайна задает повышенный стандарт защиты и узкий круг получателей, но не заменяет основания обработки и уведомления

Ирония: записная книжка в телефоне с пометкой "Свидетель по делу Петрова, не брать трубку после 22:00" - это уже обработка ПД. С риском

Один том дела - несколько режимов конфиденциальности

Что лежит в портфеле адвоката: у каждого слоя свои правила хранения и ответственность за слив

Privacy Advocates

Портфель адвоката

режимы тайн действуют параллельно закону о ПД, а не поглощаются им, поэтому один том дела живет по нескольким правилам сразу

Персональные данные

доверителя, его оппонентов, свидетелей и третьих лиц

Адвокатская тайна

все, что стало известно в связи с оказанием юридической помощи

Унаследованные тайны

банковская, врачебная, коммерческая, налоговая, иногда государственная

Ирония: адвокат законно собирает дома досье, за которое любой другой получил бы статью. Вопрос лишь в том, где это "дома" и не синхронизируется ли оно с облаком в другой юрисдикции

Разъяснение ФПА 2025 года сняло спор адвокатуры о статусе оператора

От исключения в практике ВС РФ 2011 года к разъяснению Совета ФПА от 01.07.2025

Privacy Advocates

2011

ВС РФ

Уведомление не требовалось

постановление от 05.08.2011 № 20-АД11-3 отнесло деятельность адвоката к исключению, производство по ст.19.7 КоАП прекращено

2012

РОСКОМНАДЗОР

Адвокат - оператор

позицию публиковало территориальное управление Роскомнадзора

Сегодня

152-ФЗ

Особого статуса нет

закон не выделяет адвокатов среди операторов, а профессиональная обработка чужих данных делает оператором

01.07.2025

СОВЕТ ФПА

Позиция сообщества

разъяснение разобрало уведомление Роскомнадзора, согласие физлиц и адвокатскую тайну, оно действует и для адвокатских кабинетов

Доверители

их данные и данные участников судопроизводства обрабатываются в силу закона, без согласия

Безопасность

защита данных доверителей определяется законодательством об адвокатской тайне

Работники

их данные адвокат обрабатывает как работодатель по ст.86 ТК, вне юрпомощи по разъяснению ФПА с согласием

Уведомление

подается по общему правилу, без него можно лишь при обработке без средств автоматизации

Ирония: двадцать лет адвокатура спорила, оператор ли она. Пока спорили, законодатель ввел штрафы за неуведомление об обработке ПД: адвокату как гражданину до 10 тыс. ₽, руководителю коллегии или бюро до 50 тыс. ₽

33.2

Где хранится и чем пользуемся

- Локализация: данные доверителей записывают в базы в России
- Зарубежная почта и мессенджеры - это трансграничная передача

Локализация: данные доверителей записывают в базы в России

Ч.5 ст.18 152-ФЗ в редакции 23-ФЗ от 28.02.2025 действует с 01.07.2025

Privacy Advocates

23-ФЗ

Ч.5 СТ.18 152-ФЗ

С 01.07.2025 запрет, а не условие

запись, систематизация, хранение, уточнение и извлечение ПД граждан РФ через базы за пределами России не допускаются, кроме узких исключений

- норма сформулирована как безличный запрет, а не как обязанность одного оператора
- договоры, заключенные до 01.07.2025, стоит проверить на условие о локализации

ПРАКТИЧЕСКИЙ ВОПРОС

Где физически стоят серверы вашего облака?

iCloud | Google Drive | Notion | Gmail | Outlook | заметки в телефоне

- ✕ первичная запись за рубежом с последующей репликацией в Россию с 01.07.2025 запрещена
- ✕ параллельный сбор в российскую и зарубежную базы тоже запрещен

Ирония: у меня все в облаке, то есть я не знаю, где именно, но мне там удобно - это не ответ на вопрос, где хранятся данные

Зарубежная почта и мессенджеры - это трансграничная передача

Режим локализации тянет данные в Россию, а удобные инструменты - за ее пределы

Privacy Advocates

Удобно

Чем пользуется адвокат

- Gmail и Outlook на зарубежных серверах
- переписка в иностранных мессенджерах
- заметки в телефоне и флешки
- личный ноутбук без шифрования

vs

Обязательно

Что требует закон

- передача данных за рубеж - трансграничная передача по ст.12 152-ФЗ
- с 01.03.2023 об этом отдельно уведомляют Роскомнадзор
- оценка уровня защиты ПД в стране-получателе
- первичный сбор - только в базы в России по ч.5 ст.18

Почта, мессенджеры и ВКС

скачать

РОСКОМНАДЗОР, ПИСЬМА ОТ 24.03.2025 И 10.04.2025

ч.5 ст.18 в редакции 23-ФЗ запрещает **сбор** с использованием зарубежных баз, но не ограничивает ТПД данных, уже собранных в российских базах: для нее действуют ст.12 и уведомление о намерении

Ирония: адвокатская тайна, отправленная через мессенджер с серверами на другом континенте, защищена сквозным шифрованием (нет). Зато стикеры красивые

33.3

Цена вопроса и первые шаги

- Цена вопроса: не оборотный штраф, но и не шутка
- Оценка рисков в понедельник утром: пять шагов

Цена вопроса: не оборотный штраф, но и не шутка

Административная, уголовная и дисциплинарная ответственность адвоката за ПД и тайну

Privacy Advocates

КоАП, ст.13.11

Адвокат отвечает как гражданин

- оборотные штрафы 1-3% выручки до 500 млн ₽ к нему неприменимы (ред. 420-ФЗ с 30.05.2025)
- за утечку гражданину по чч.12-14 до 400 тыс. ₽, применение к адвокату спорно, за коллегию и бюро как НКО отвечают должностные лица, до 600 тыс. ₽
- за нелокализацию по ч.8 и 9 до 50 тыс. ₽ и до 100 тыс. ₽ при повторности

УК, ст.272.1

Незаконный оборот ПД

- незаконные сбор, хранение, использование или передача компьютерной информации с ПД
- действует с 11.12.2024 (421-ФЗ)
- вплоть до лишения свободы

63-ФЗ и КПЭА

Дисциплинарная ответственность

- за нарушение адвокатской тайны (ст.8 63-ФЗ, ст.6 Кодекса профессиональной этики адвоката)
- то, чего деньгами не закрыть

Хорошая новость: штраф в 500 млн ₽ придуман не для адвоката. Плохая: по ст.272.1 УК можно поменяться с доверителем ролями - из защитника в подзащитного

Оценка рисков в понедельник утром: пять шагов

Инвентаризация рисков отличает разумные меры от "я об этом не думал"

Privacy Advocates

1

Где данные

понять, где физически хранятся клиентские данные, и взвесить иностранную инфраструктуру против отечественной

2

Железо

оценить уязвимости: незашифрованный ноутбук, общий личный и рабочий аккаунт, флешки

3

Инцидент

проверить политику обработки ПД, формы согласий и сроки реакции: уведомить Роскомнадзор об утечке за 24 и 72 часа

4

Уведомления

взвесить риски подачи и неподачи уведомления об обработке с учетом разъяснения ФПА 2025 года, а также риски ТПД

5

Режим письменно

зафиксировать режим обращения с информацией, чтобы подтвердить разумные меры

Дальше: порядок уведомлений об утечке разобран в разделе 28 "Инциденты", а чек-лист основных контролей обработки и защиты ПД - в разделе ресурсов

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
FIN-001	Чек-лист из основных контролей обработки и защиты ПД	Ресурсы и контакты

34

ПД в процедуре банкротства

Шесть критериев допустимости в процедуре банкротства

34.1 Шесть критериев в процедуре банкротства

34.2 Особенности режима и риски

Раздел на сайте
privacy-advocates.ru/pd/bnk

34.1

Шесть критериев в процедуре банкротства

- Сведения о должнике остаются ПД и после публикации в ЕФРСБ
- Цели обработки в банкротстве задает закон, а не управляющий
- Раскрывают только сведения из ст.213.7, запрашивают лишь нужное
- Согласие должника не нужно: основания обработки дает закон

Сведения о должнике остаются ПД и после публикации в ЕФРСБ

Предметность в процедуре банкротства: п.5 ст.213.7 127-ФЗ

Privacy Advocates

Состав ПД в деле о банкротстве **заведомо широк**, а презумпция предметности сохраняется: сведения, прямо или косвенно определяющие должника и связанных лиц, остаются ПД, даже став общедоступными в ЕФРСБ

Должник-гражданин

ФИО, дата и место рождения, СНИЛС, ИНН, место жительства (п.5 ст.213.7), у предпринимателя также ОГРНИП

Имущество и обязательства

имущество, доходы, банковские счета, сделки, кредиторы и обязательства должника

Связанные лица

члены семьи, контролирующие должника лица, контрагенты по оспариваемым сделкам

Финансовый управляющий

его ФИО, ИНН, СНИЛС и адрес тоже подлежат опубликованию

Критерий 1 из 6, предметность: любые сведения о человеке - ПД, пока прямо не доказано обратное (п.1 ст.3 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Цели обработки в банкротстве задает закон, а не управляющий

Целенаправленность в процедуре банкротства: п.5 ст.213.7 и ст.20.3 127-ФЗ

Privacy Advocates

Конкретные законные цели предопределены законом о банкротстве

1. формирование конкурсной массы и расчеты с кредиторами
2. публичность и прозрачность процедуры через опубликование сведений в ЕФРСБ
3. выявление, анализ и оспаривание сделок должника, розыск его имущества
4. идентификация должника при каждом опубликовании, обязательная в силу ст.213.7

ЦЕЛИ ЗАДАНЫ ИМПЕРАТИВНО

Ни шире, ни уже

финансовый управляющий не вправе ни расширить, ни сузить цели по своему усмотрению. Обработка ПД вне целей процедуры недопустима

- требование должника прекратить обработку опубликованных сведений не удовлетворяется, пока обработка не выходит за цель раскрытия
- агрегирование публикаций о банкротстве в коммерческий продукт выходит за эту цель и требует собственного основания

Критерий 2 из 6, целенаправленность: цели конкретны, определены заранее и законны, новая цель совместима с исходной (ч.2 ст.5 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Раскрывают только сведения из ст.213.7, запрашивают лишь нужное

Пропорциональность в процедуре банкротства: ст.213.7, 28 и 20.3 127-ФЗ

Privacy Advocates

Публикация

Только перечень ст.213.7

- ст.213.7 специальна по отношению к ст.28 (определение ВС РФ от 25.02.2020 № 309-ЭС19-15908)
- сведения, не названные в ст.213.7, не публикуют, даже если они есть в ст.28
- по делам граждан публикация в ЕФРСБ, в "Коммерсанте" - только о признании заявления обоснованным и о реализации имущества

Истребование

Только нужное для процедуры

- запросы управляющего по ст.20.3 ограничены данными о должнике, КДЛ, контрагентах и имуществе
- с 29.05.2024 сведения об имуществе, счетах и вкладах должника и его супруга запрашивают без суда (абз.5 п.7 ст.213.9)
- отказать можно, если запрос с очевидностью не связан с конкурсной массой, а переписку истребуют только через суд

Критерий 3 из 6, пропорциональность: минимизация состава, раздельное хранение и отказ от накопления "на всякий случай" (чч.3-7 ст.5 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Согласие должника не нужно: основания обработки дает закон

Легальность в процедуре банкротства: ст.213.7 127-ФЗ и ч.1 ст.6 152-ФЗ

Privacy Advocates

ОСНОВАНИЕ, Ч.1 СТ.6 152-ФЗ	ЧТО ПОКРЫВАЕТ В БАНКРОТСТВЕ
п.2	функции, полномочия и обязанности, возложенные законом на управляющего, СРО и суд
п.11	обязательное опубликование и раскрытие ПД, прямо названное в ст.213.7 127-ФЗ
п.3	участие в судопроизводстве и исполнительном производстве

СТ.10.1 НЕ ПРИМЕНЯЕТСЯ

идентифицирующие сведения должника в судебных актах по банкротству - обязательное раскрытие, а не распространение по согласию (Девятнадцатый ААС, 15.01.2025, А14-12999/2024)

СТАТУС ОПЕРАТОРА

Управляющий - самостоятельный оператор

- по ст.22 152-ФЗ по общему правилу уведомляет Роскомнадзор до начала обработки
- отзыв согласия неприменим, раз обработка идет не на согласии
- статус не освобождает от ответа субъекту по ст.14: так указал Третий КСОЮ 07.07.2025 (№ 16-2744/2025), хотя дело прекратил за давностью

Критерий 4 из 6, легальность: основной квартет оснований - пп.1, 2, 5, 7 ч.1 ст.6 152-ФЗ, вспомогательный квинтет - пп.3, 3.1, 6, 8, 9. Общий критерий - в разделе 06 "Допустимость обработки"

Публичность банкротства ограничивает приватность должника

Транспарентность в процедуре банкротства: ст.28 и 213.7 127-ФЗ

Privacy Advocates

ОСОБЕННОСТЬ РЕЖИМА

ЕФРСБ и "Коммерсантъ"

сведения о банкротстве общедоступны в ЕФРСБ (Федресурс), часть сообщений - в газете

Идентификация

при каждом опубликовании обязательны ФИО, дата рождения, ИНН, СНИЛС, место жительства, поэтому должника легко найти

Нет полной тайны

полная конфиденциальность личной информации должника невозможна из-за публичного характера процедуры

РАЗУМНОЕ ОЖИДАНИЕ

Раскрытие - законное следствие

вступая в процедуру, гражданин информируется о неизбежном раскрытии его ПД неограниченному кругу лиц. Так ожидание субъекта совпадает с обработкой

Критерий 5 из 6, транспарентность: субъект знает об обработке до ее начала и может разумно ее ожидать (чч.1-2 ст.14 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Защита ПД должника не отменяет обязательного раскрытия

Безопасность в процедуре банкротства: п.3 ст.20.3 127-ФЗ и ст.19 152-ФЗ

Privacy Advocates

Конфиденциальность

управляющий хранит конфиденциальность охраняемых законом сведений, ставших известными при исполнении обязанностей (п.3 ст.20.3)

Доступ по основанию

ПД должника доступны только лицам с законным основанием: арбитражному суду, кредиторам, арбитражному управляющему

Меры по ст.19

распространяются на управляющего, СРО, организатора торгов и оператора электронной площадки

БАЛАНС

Ограждаются лишь избыточные сведения

защита ПД не отменяет раскрытия по ст.213.7, закрываются только сведения, не подлежащие опубликованию

ПРАКТИКА

Обезличенная выдача вместо отказа

Девятый ААС 28.09.2020 по делу № А40-79738/2018 обязал управляющего выдать кредитору сведения о выплатах работникам в обезличенной форме

Критерий 6 из 6, безопасность: классическая ИБ из 30+ подсистем, обезличивание обратимо и не прекращает обработку (ст.7 и 19 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
DOP-003	Базовые критерии допустимости обработки ПД	06 Допустимость
DOP-004	Предметность: ПД бывают в любой сфере жизни человека	06 Допустимость
DOP-005	Целенаправленность	06 Допустимость
DOP-006	Пропорциональность (целесообразность)	06 Допустимость
DOP-007	Легальность	06 Допустимость
DOP-008	Транспарентность	06 Допустимость
DOP-009	Безопасность	06 Допустимость

34.2

Особенности режима и риски

- Банкротство - принудительная публичность без права на забвение

Банкротство - принудительная публичность без права на забвение

Резюме: особенности режима ПД в процедуре банкротства и его риски

Privacy Advocates

Особенности режима

- принудительная публичность: раскрытие в ЕФРСБ и "Коммерсанте" - не выбор, а обязанность по 127-ФЗ
- обработка без согласия должника по пп.2, 3, 11 ч.1 ст.6 152-ФЗ, отзыв согласия неприменим
- множество операторов: финансовый управляющий, СРО, организатор торгов, ЭТП, оператор ЕФРСБ, суд
- минимизация только в коридоре ст.213.7, специальной к ст.28 по позиции ВС РФ

Проблематика и риски

- бессрочность публикаций: завершение процедуры не влечет удаления, права на забвение нет
- ПД семьи, КДЛ и контрагентов обрабатываются и публикуются без их согласия и уведомления
- размыты роли и ответственность операторов и режим поручения обработки площадкам
- спорная выдача ПД по запросам ст.20.3 127-ФЗ и неустойчивая практика госорганов

Риск для держателей данных: отказ конкурсному управляющему в сведениях со ссылкой на 152-ФЗ суды признают поводом для дела по ч.4 ст.14.13 КоАП (АС Московского округа, А41-10789/2018)

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
FIN-001	Чек-лист из основных контролей обработки и защиты ПД	Ресурсы и контакты
OTV-003	Ландшафт юридической ответственности за ПД	30 Ответственность

35

ПД в фармаконадзоре

Шесть критериев допустимости в фармаконадзоре

Раздел на сайте
privacy-advocates.ru/pd/frm

Сообщение о нежелательной реакции - уже ПД спецкатегории

Предметность в фармаконадзоре: ст.64 61-ФЗ, Правила GVP ЕАЭС, ст.10 152-ФЗ

Privacy Advocates

ЧЕТЫРЕ ЭЛЕМЕНТА ВАЛИДНОГО СООБЩЕНИЯ О НР

Репортер

идентифицируемый источник: квалификация, имя или инициалы, адрес или контакты

Пациент

хватит одного признака: инициалы, номер медкарты, дата рождения, возраст, пол

Препарат

подозреваемый лекарственный препарат

Реакция

сама нежелательная реакция

Данные о здоровье и НР - **специальная категория ПД** (ст.10 152-ФЗ), а формально обезличенный кейс восстановим по связке дата, пол, возраст, анамнез

ВЫВОД

- сообщение о НР по умолчанию содержит ПД, в том числе специальной категории
- анонимность отдельного кейса, как правило, мнимая
- минимальный валидный кейс - 4 элемента
- **Опора:** Правила GVP ЕАЭС, пп.385, 407

Критерий 1 из 6, предметность: любые сведения о человеке - ПД, пока прямо не доказано обратное (п.1 ст.3 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Цель фармаконадзора задает закон, а не держатель РУ

Целенаправленность в фармаконадзоре: ст.64 61-ФЗ и Правила GVP ЕАЭС

Privacy Advocates

Цель предопределена законом, а не оператором

- обеспечение безопасности ЛП и контроль соотношения ожидаемой пользы и возможного вреда (ст.64 61-ФЗ)
- цель конкретна, законна и общественно значима - защита жизни и здоровья населения

ИНАЧЕ ЦЕЛЬ НЕ ДОСТИЧЬ: ИДЕНТИФИЦИРУЕМОСТЬ НУЖНА ДЛЯ

1. **Верификации** — проверка сообщений и устранение дублей
2. **Follow-up** — запрос дополнительной информации у репортера
3. **Оценки** — причинно-следственная связь и серьезность НР

ВЫВОД

- цель задает закон, а не усмотрение оператора
- обезличить данные на входе нельзя, иначе кейс непригоден для оценки безопасности
- **Опора:** ст.64 61-ФЗ, Правила GVP ЕАЭС

Критерий 2 из 6, целенаправленность: цели конкретны, определены заранее и законны, новая цель совместима с исходной (ч.2 ст.5 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Минимум данных в фармаконадзоре - это валидный случай

Пропорциональность: Правила GVP ЕАЭС № 87, ст.5 и ч.3 ст.6 152-ФЗ

Privacy Advocates

1. **Минимизация, но не ниже обязательного минимума**
   4 элемента валидного сообщения о НР собираются всегда, иначе кейс недействителен. Собирают только релевантный анамнез, без накопления данных "на всякий случай"

2. **Раздельное хранение и кодирование**
   идентификаторы репортера и пациента отделяют от медицинских сведений: псевдонимизация, код кейса

3. **Точечное привлечение третьих лиц**
   колл-центры и поставщики IT-систем - по поручению и под контролем, число таких эпизодов лучше минимизировать: ответственность остается на держателе РУ

ВЫВОД

- минимум данных = минимум валидного кейса
- поручение третьим лицам - точечно и под контролем оператора
- **Опора:** Правила GVP ЕАЭС, ст.5 и ч.3 ст.6 152-ФЗ

Критерий 3 из 6, пропорциональность: минимизация состава, раздельное хранение и отказ от накопления "на всякий случай" (чч.3-7 ст.5 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Фармаконадзор идет по закону, без письменного согласия

Легальность: п.2 ч.1 и ч.3 ст.6 152-ФЗ, ст.64 61-ФЗ, письма Роскомнадзора ноября 2025 года

Privacy Advocates

обработка фармацевтическими компаниями персональных данных во исполнение федеральных законов, подзаконных актов, а также Правил надлежащей практики фармаконадзора ЕАЭС от 03.11.2016 № 87 подпадает под правовые основания, предусмотренные п. 2 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и не требует получения согласия субъекта персональных данных в письменной форме

Письмо Роскомнадзора от 25.11.2025 № 08-604997

ТРЕТЬИ ЛИЦА

колл-центры и IT-поставщики - поручение по ч.3 ст.6 152-ФЗ

ЗА ПЕРИМЕТРОМ ФН

маркетинг, иные контакты с субъектом и действия вне GVP и мастер-файла требуют иного основания, в том числе согласия

СПОРНО

в ч.2 ст.10 нет основания "исполнение закона", а анамнез - спецкатегория

Критерий 4 из 6, легальность: основной квартет оснований - пп.1, 2, 5, 7 ч.1 ст.6 152-ФЗ, вспомогательный квинтет - пп.3, 3.1, 6, 8, 9. Общий критерий - в разделе 06 "Допустимость обработки"

О фармаконадзоре информируют доступными каналами

Транспарентность: ст.14 и 18 152-ФЗ, Правила GVP ЕАЭС

Privacy Advocates

Прямое информирование затруднено

сообщение о НР часто приходит от медработника или родственника, пациент может быть недоступен

Управление ожиданиями

обработка сообщений о НР ради безопасности ЛП - разумно ожидаемая деятельность держателя РУ

Исключение

сообщение по обязанности из закона подпадает под п.2 ч.4 ст.18, иначе каналы лишь снижают риск по ч.3 ст.18

КАНАЛЫ ИНФОРМИРОВАНИЯ

- политика обработки ПД
- инструкция по применению
- сайт держателя РУ
- форма сообщения о НР
- слово репортеру при приеме

ВЫВОД

- информируем доступными каналами с учетом источника данных
- цель - оправданные ожидания и доверие субъекта ПД
- **Опора:** ст.14 152-ФЗ, Правила GVP ЕАЭС

Критерий 5 из 6, транспарентность: субъект знает об обработке до ее начала и может разумно ее ожидать (чч.1-2 ст.14 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Псевдонимизация вместо обезличивания по приказу № 140

Безопасность: ст.19 152-ФЗ, приказ Роскомнадзора от 19.06.2025 № 140, Правила GVP ЕАЭС

Privacy Advocates

Спецкатегория
повышенные меры защиты по ст.19

Коды кейсов
анонимизация неприменима: теряется прослеживаемость кейса

Доступ
уполномоченное лицо по ФН и профильные специалисты

Поручение и ТПД
колл-центры, IT-поставщики, глобальные базы - по 152-ФЗ

ПРИКАЗ № 140

Формальное обезличивание - сущая морока

нужны отдельные ЛНА, раздельное хранение исходных и обезличенных данных и учет всех действий. Разумнее применять псевдонимизацию, кодирование и декомпозицию как меры защиты

ВЫВОД

- не обезличивание, а псевдонимизация
- защита спецкатегории при сохранении прослеживаемости кейса
- методики обезличивания без формальной обвязки приказа № 140
- **Опора:** ст.19 152-ФЗ, приказ Роскомнадзора № 140, GVP ЕАЭС

Критерий 6 из 6, безопасность: классическая ИБ из 30+ подсистем, обезличивание обратимо и не прекращает обработку (ст.7 и 19 152-ФЗ). Общий критерий - в разделе 06 "Допустимость обработки"

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
DOP-003	Базовые критерии допустимости обработки ПД	06 Допустимость
DOP-004	Предметность: ПД бывают в любой сфере жизни человека	06 Допустимость
DOP-005	Целенаправленность	06 Допустимость
DOP-006	Пропорциональность (целесообразность)	06 Допустимость
DOP-007	Легальность	06 Допустимость
DOP-008	Транспарентность	06 Допустимость
DOP-009	Безопасность	06 Допустимость
FIN-001	Чек-лист из основных контролей обработки и защиты ПД	Ресурсы и контакты
OTV-003	Ландшафт юридической ответственности за ПД	30 Ответственность

ЧАСТЬ

X

Тайны и защита информации

Коммерческая тайна, служебная информация и система защиты информации

36 Комплаенс в области защиты информации

37 Режим коммерческой тайны

36

Комплаенс в области защиты информации

Режимы ограничения доступа, КТ, система ИБ, DLP и переписка

36.1 Режимы ограничения доступа

36.2 КТ и служебная информация

36.3 Система управления ИБ

36.4 Мониторинг персонала и DLP

36.5 Решение кейса и источники

36.6 Переписка и тайна связи

Раздел на сайте
privacy-advocates.ru/pd/zin

36.1

Режимы ограничения доступа

В этой части

- Тайну защищают режим, процессы и доказательства
- Кейс Альфа-Софт проверяет режим КТ, инсайд и DLP
- Доступ ограничивают в силу закона или по решению обладателя
- В законах РФ более 50 тайн с разными режимами

Тайну защищают режим, процессы и доказательства

Цена ошибки в цифрах 2025-2026 годов и главный вопрос раздела

Privacy Advocates

Ключевой менеджер ушел к конкуренту вместе с базой клиентов. **Получится ли доказать в суде, что это была коммерческая тайна?**

500 млн ₽

Оборотный штраф

максимум за повторную утечку ПД с 30.05.2025, от 1 до 3% выручки (ст.13.11 КоАП)

100+

Утечек баз ПД в 2025 году

по данным Роскомнадзора, десятки миллионов записей. В I полугодии 2026 года выявлено еще 12

большинство

Компаний контролируют персонал

по опросу 2025 года, примерно каждая шестая следит за активностью работников на компьютерах

6

Случаев инсайда

выявил Банк России с начала 2025 года к августу, чаще всего это топ-менеджеры

Тезис: информация защищена ровно настолько, насколько компания смогла оформить режим, выстроить процессы и собрать доказательства

Кейс Альфа-Софт проверяет режим КТ, инсайд и DLP

Вымышленная ИТ-компания: 300 сотрудников, SaaS для ритейла, облигации на бирже

Privacy Advocates

1 **Эпизод 1. Разработчик ушел с кодом**

перед увольнением выгрузил исходный код и базу клиентов в личное облако и перешел к конкуренту. В трудовом договоре есть пункт о неразглашении, но перечня сведений КТ (коммерческая тайна) и Положения о режиме нет

2 **Эпизод 2. Финансовый директор продал облигации**

узнал о срыве крупного контракта, до публикации новости продал облигации компании и посоветовал брату поступить так же

3 **Эпизод 3. DLP (система предотвращения утечек) читает все мессенджеры**

руководство купило систему, которая делает скриншоты каждые 5 минут и читает мессенджеры на рабочих ноутбуках. Сотрудникам решили не сообщать, чтобы поймать нарушителей

ОТВЕТИМ В КОНЦЕ РАЗДЕЛА

Четыре вопроса кейса

1. можно ли уволить разработчика и взыскать убытки
2. какой режим выбрать для архитектуры и внутренних регламентов
3. нарушил ли финансовый директор 224-ФЗ
4. законен ли такой мониторинг и как его исправить

Доступ ограничивают в силу закона или по решению обладателя

Ст.5 149-ФЗ делит информацию на общедоступную и ограниченного доступа

Privacy Advocates

ст.9 149-ФЗ

В силу федерального закона

- только федеральный закон ограничивает доступ, чтобы защитить права других лиц, здоровье, нравственность, оборону и безопасность
- соблюдать конфиденциальность обязан каждый, кто получил доступ
- например, ПД, банковская и врачебная тайна, инсайд, гостайна
- с гостайной работают только по лицензии и с допуском (закон РФ О государственной тайне)

или

п.1 ч.3 ст.6 149-ФЗ

По решению обладателя

- обладатель вправе разрешать или ограничивать доступ и определять его условия, если закон не запрещает
- инструменты - режим КТ (коммерческая тайна) по 98-ФЗ или режим информации для внутреннего пользования (ИВП)
- нельзя закрыть сведения из ч.4 ст.8 149-ФЗ и ст.5 98-ФЗ

Правило. Тайну образуют три элемента закона: перечень сведений, меры ограничения доступа и ответственность. Самоназвание тайной во внутреннем документе режима не создает

Служебная тайна в строгом смысле есть только у госорганов и подведомственных им организаций, это сведения с пометкой ДСП (Указ Президента РФ № 188, постановление Правительства РФ № 1233). Аналог в коммерческой компании - ИВП

В законах РФ более 50 тайн с разными режимами

У каждой тайны свой закон, свой круг обязанных лиц и своя ответственность

Privacy Advocates

Тайны о человеке

ПД, врачебная тайна, личная и семейная тайна, тайна усыновления, завещания, исповеди, голосования, тайна связи

Профессиональные тайны

адвокатская, нотариальная, аудиторская, банковская и налоговая тайна, тайна страхования, медиации, арбитража, кредитных историй, пенсионная тайна

Бизнес и финансовый рынок

коммерческая тайна и ноу-хау, инсайдерская информация, клиринговая тайна, тайна организованных торгов, тайна корпоративного договора

Государство и правосудие

государственная тайна, служебная тайна (ДСП), тайна следствия, тайна совещания судей, тайна ОРД, таможенная тайна

Безопасность и инфраструктура

безопасность КИИ, тайна обеспечения ИБ (информационная безопасность), сведения о защищаемых лицах, паспорта безопасности объектов ТЭК

ИВП - не тайна по закону

режим, который обладатель вводит сам по ст.6 149-ФЗ, без закона о тайне и без его ответственности

Тайны различаются механизмом: по содержанию сведений (гостайна, КТ (коммерческая тайна)), по сфере деятельности (врачебная, адвокатская, банковская тайна) и особая сфера частной жизни. Поэтому проверяют по перечню, по источнику получения или по характеру сферы

Одна запись бывает ПД, КТ и инсайдом одновременно

Как соотносятся режимы: основание, кто вводит и какая ответственность

Privacy Advocates

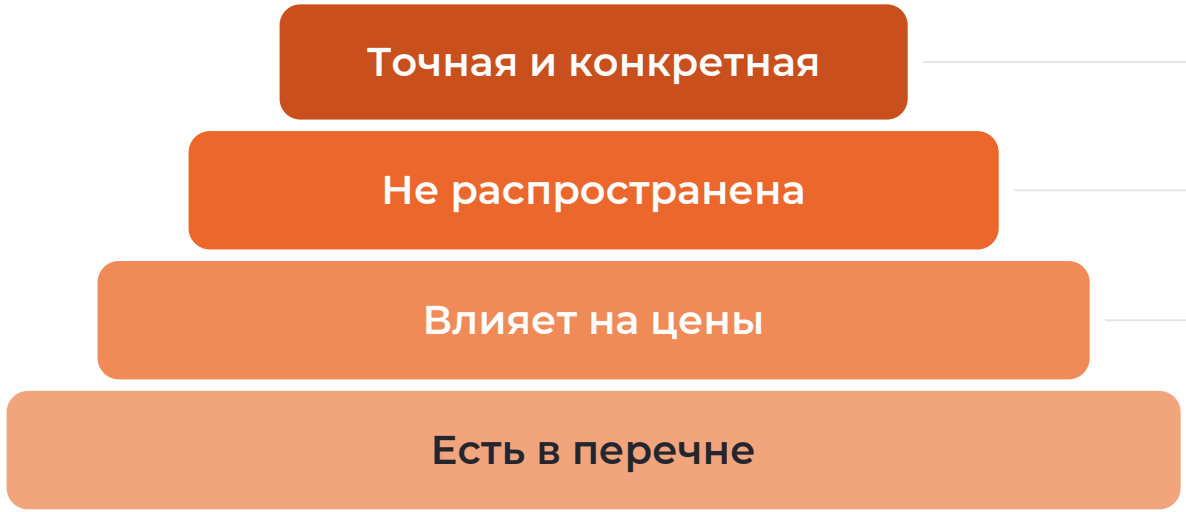
РЕЖИМ	ОСНОВАНИЕ	КТО ВВОДИТ И ДЛЯ КОГО	ОТВЕТСТВЕННОСТЬ
Персональные данные	152-ФЗ	закон, для всех операторов ПД	ст.13.11 КоАП с оборотными штрафами, ст.137 и 272.1 УК
Коммерческая тайна	98-ФЗ, ст.1465 ГК	обладатель, если выполнил меры ст.10 98-ФЗ	увольнение, полная материальная ответственность, ст.13.14 и 14.33 КоАП, ст.183 УК
Профессиональные тайны	законы о банках, медицине, адвокатуре, нотариате, связи	закон, для профессионалов и их работников	отраслевая, ст.13.14 КоАП, ст.137, 138, 183 УК
Инсайдерская информация	224-ФЗ	закон, для эмитентов, профучастников и инсайдеров	ст.15.21 и 15.35 КоАП, ст.185.6 УК
Служебная тайна (ДСП)	постановление Правительства РФ № 1233	госорганы и подведомственные организации	дисциплинарная
Информация для внутреннего пользования	ч.3 ст.6 149-ФЗ, ЛНА (локальные нормативные акты), договоры	обладатель по своему решению	**дисциплинарная и договорная**

Режимы накладываются: база клиентов бывает одновременно ПД и КТ (коммерческая тайна), а прогноз выручки до раскрытия - КТ и инсайдом. Требования применяют в совокупности, при расхождении - самые строгие

Инсайд есть, только если выполнены все четыре признака

Признаки инсайдерской информации по п.1 ст.2 224-ФЗ и круг инсайдеров по ст.4

Privacy Advocates



- **Точная и конкретная** — определенные сведения, а не слухи и оценки
- **Не распространена** — не была распространена или предоставлена, в том числе КТ (коммерческая тайна) и иная тайна
- **Влияет на цены** — может существенно повлиять на цены финансовых инструментов, валюты или товаров
- **Есть в перечне** — входит в перечень инсайдерской информации по ст.3 224-ФЗ

Кто инсайдер, ст.4

- эмитенты и управляющие компании
- биржи, клиринг, брокеры, депозитарии, банки
- члены советов директоров, исполнительных органов, ревизоры
- владельцы не менее 25% голосов
- аудиторы, оценщики, консультанты, рейтинговые агентства
- работники и подрядчики с доступом по договору

Важно: инсайд может одновременно быть КТ, банковской или иной тайной, это прямо сказано в определении. После раскрытия сведения перестают быть инсайдом

Инсайд создает обязанности эмитенту и запреты инсайдерам

Чек-лист эмитента по ст.3, 8-11 224-ФЗ, запреты ст.6, ответственность и практика Банка России

Privacy Advocates

- утвердить и раскрыть перечень инсайдерской информации (ст.3)
- вести список инсайдеров, уведомлять о включении и исключении (ст.9)
- назначить ответственное должностное лицо или подразделение (ст.11)
- утвердить правила доступа к инсайду и внутреннего контроля (ст.11)
- раскрывать инсайдерскую информацию в установленные сроки (ст.8)
- запрашивать у инсайдеров сведения об их сделках (ст.10)

ЗАПРЕЩЕНО ИНСАЙДЕРУ, СТ.6

- сделки на основе инсайда
- передача инсайда без основания
- рекомендации и побуждение к сделкам
- манипулирование рынком

ОТВЕТСТВЕННОСТЬ

- ст.15.21 КоАП - использование инсайда
- ст.15.35 КоАП - нарушения эмитента
- ст.185.6 УК - крупный ущерб или доход
- законопроект № 1075257-8 (I чтение 11.02.2026, идет ко II): закрытые периоды для сделок инсайдеров

Практика Банка России, 2025: член совета директоров ПАО Ашинский метзавод купил акции в день заседания о дивидендах и продал с прибылью после раскрытия. Итог - административная ответственность и предписание

Режим выбирают под каждый массив информации

Выводы подраздела о режимах ограничения доступа

Privacy Advocates

Начните с инвентаризации. Составьте реестр информационных массивов и для каждого укажите **режим, владельца и круг лиц с доступом**

Алексей Мунтян, рекомендация эксперта

ВЫВОДЫ

1. ограничить доступ можно в силу закона или по решению обладателя, для каждого массива нужен свой режим
2. режимы пересекаются, одна запись бывает ПД, КТ (коммерческая тайна) и инсайдом сразу, поэтому применяют самые строгие требования
3. инсайд касается не только бирж, если облигации компании торгуются на бирже, 224-ФЗ уже применяется

36.2

КТ и служебная информация

В этой части

- КТ возникает только при четырех признаках одновременно
- Сведения из ст.5 98-ФЗ не станут КТ даже с грифом
- Режим КТ установлен только после всех пяти мер
- В перечень КТ Альфа-Софт входит только ценное

КТ возникает только при четырех признаках одновременно

Признаки ст.3 98-ФЗ и ч.1 ст.1465 ГК: без секретности и ценности нет охраны

Privacy Advocates

01

Коммерческая ценность

действительная или потенциальная, в силу неизвестности

02

Неизвестность

сведения неизвестны третьим лицам

03

Нет свободного доступа

на законном основании

04

Введен режим КТ

обладатель принял меры ст.10 98-ФЗ

ПРАКТИКА СИП, 2026

Ноу-хау из шаблонов

лицензиат заплатил 1 млн ₽ за секрет производства, эффективную бизнес-модель агентства недвижимости. Это оказались общедоступные шаблоны и типовые материалы. Суд по интеллектуальным правам (постановление от 30.04.2026 № С01-322/2026) указал, что секретности и ценности нет, значит нет и охраны

Учесть: сведения бывают любого характера, производственные, технические, экономические, организационные, в том числе о результатах интеллектуальной деятельности. Признаки проверяют по каждой позиции перечня отдельно

Сведения из ст.5 98-ФЗ не станут КТ даже с грифом

Что нельзя сделать коммерческой тайной: 11 категорий в четырех группах

Privacy Advocates

11

СТ.5 98-ФЗ

категорий сведений не могут составлять КТ

суд не признает их КТ, даже если на них стоит гриф

О компании

учредительные документы и записи в госреестрах, разрешения на деятельность, лица, действующие без доверенности

О работниках

численность и состав, система оплаты и условия труда, травматизм, вакансии, долги по зарплате

О безопасности

загрязнение среды, пожарная безопасность, санитарно-эпидемиологическая и радиационная обстановка, безопасность продуктов

Прочее

нарушения закона и привлечение к ответственности, имущество госпредприятий и НКО, приватизация, сведения с обязательным раскрытием

Отмененный перечень

постановление Правительства РСФСР от 05.12.1991 № 35 (бухотчетность, налоги, платежеспособность) утратило силу с 26.07.2025, остался перечень ст.5 98-ФЗ

Практический вывод: систему оплаты труда скрыть нельзя, а зарплату конкретного работника защищает режим ПД (152-ФЗ, ст.88 ТК)

Режим КТ установлен только после всех пяти мер

Меры ч.1 ст.10 98-ФЗ и документы, которыми их подтверждают

Privacy Advocates

1

Перечень сведений

приказ об утверждении перечня сведений, составляющих КТ (коммерческая тайна)

2

Порядок обращения и контроль

Положение о режиме КТ, назначение ответственного

3

Учет лиц с доступом

перечень должностей с доступом, журналы учета лиц и носителей

4

Договоры

обязательство о неразглашении для работников, NDA с контрагентами

5

Гриф на носителях

Коммерческая тайна с наименованием и местом нахождения обладателя, в том числе в шаблонах файлов

Пропуск любой меры означает, что режима нет: ни убытков, ни увольнения за разглашение, ни уголовной защиты. Меры разумно достаточны, если исключают доступ без согласия обладателя (ч.5 ст.10)

Плюс ст.11 98-ФЗ: ознакомьте работника под подпись с перечнем, режимом и мерами ответственности и создайте условия для соблюдения режима. Нет подписи, нет и ответственности. Даты актов, расписок и грифа фиксируйте документально

В перечень КТ Альфа-Софт входит только ценное

Применяем алгоритм к кейсу: что включить в перечень, а что оставить за его рамками

Privacy Advocates

Включаем в перечень КТ

- исходный код ядра платформы и непубличные алгоритмы
- архитектура продукта и план развития до анонса
- база клиентов с условиями договоров и скидками
- себестоимость и маржинальность проектов
- стратегия участия в тендерах и переговорах

Не включаем

- систему оплаты труда и численность (ст.5 98-ФЗ)
- сведения о нарушениях и штрафах
- открытый код и публичную документацию API
- пароли и ключи, это предмет политики ИБ (информационная безопасность)
- внутренние регламенты и оргструктуру, их переносим в режим ИВП (информация для внутреннего пользования)

Пишите конкретно: не вся финансовая информация, а себестоимость услуг по проектам до публикации отчетности. Ориентир - сведения, за которые конкурент готов заплатить, с обоснованием ценности по каждой позиции

Для увольнения за разглашение нужны режим КТ и доказанный вынос

Практика 2014-2026 годов: от флешки на проходной до загрузки в сервис модели

Privacy Advocates

СУД И АКТ	ЧТО СДЕЛАЛ РАБОТНИК	ИТОГ	ДОВОД СУДА
Мосгорсуд, апелляционное определение от 08.09.2014 № 33-18661/2014	отправил сведения КТ (коммерческая тайна) с рабочего места на внешний адрес	законно	раскрытие состоялось при отправке, провайдеры почты тоже третьи лица
Новгородский областной суд, апелляционное определение от 25.07.2018 № 33-1732/2018	пытался вынести флешку с программой, отнесенной к КТ, носитель изъяли на проходной	незаконно	сведения не стали известны третьим лицам, передачи не было
3 КСОЮ, определение от 15.06.2026 № 88-10469/2026	ознакомлен с Положением о КТ, скачал в личное облако и отправил на личную почту сведения о технологиях и контрагентах	законно	отправка вопреки запрету - разглашение, даже если третьи лица не видели, ущерб не нужен
Бабушкинский районный суд г. Москвы, решение от 26.05.2026 № 02-1545/2026	ставил личный адрес в скрытую копию, часть документов загрузил в DeepSeek	увольнение законно	нет производственной необходимости выносить сведения, выгрузку в сервис суд учел. Иск удовлетворен частично: замечание отменено, 10 000 ₽ морального вреда, первая инстанция

КС РФ, постановление от 26.10.2017 № 25-П: пересылка служебной информации на личную почту создает угрозу ее неконтролируемого распространения. Но довод работает, только если обладатель сам принял меры, а без положения, перечня и листов ознакомления он бесполезен

ИВП закрывает внутреннюю информацию без строгости КТ

Информация для внутреннего пользования: основание, признаки, состав и ответственность

Privacy Advocates

ПРАВОВОЕ ОСНОВАНИЕ

п.1 ч.3 ст.6 149-ФЗ
обладатель разрешает или ограничивает доступ, задает его порядок и защищает права при незаконном получении информации

ч.1 ст.1465 ГК
разумные меры конфиденциальности шире режима коммерческой тайны

ст.21 и 189 ТК
работник соблюдает локальные акты и трудовой распорядок

ЧТО ОБЫЧНО ОТНОСЯТ К ИВП

- порядок обеспечения физической, экономической и информационной безопасности
- структура сети и информационных систем
- сведения контрагентов, закрытые договором
- ход исследований и пилотных проектов
- планы встреч, совещаний, регламенты

Признаки ИВП

- сведения вне иной охраняемой тайны
- неизвестны третьим лицам
- нет свободного доступа на законном основании
- обладатель ввел режим ограничения

Ответственность: ИВП не охраняемая законом тайна, увольнения по пп.в п.6 ч.1 ст.81 ТК нет. Остаются взыскания по ст.192 ТК, при неоднократности п.5 ч.1 ст.81 ТК, с контрагентами неустойка

Режим для массива выбирают тремя вопросами

Алгоритм выбора между специальным режимом, КТ и ИВП для каждой строки реестра

Privacy Advocates

1. Доступ ограничен федеральным законом? Например, ПД, банковская тайна, инсайд

Да - действует специальный режим этого закона, КТ (коммерческая тайна) можно добавить сверху, если выполнены признаки, но основания обработки ПД она не заменяет. Нет - к вопросу 2

2. Сведения из ст.5 98-ФЗ или подлежат обязательному раскрытию?

Да - ограничить доступ нельзя, сведения должны оставаться доступными. Нет - к вопросу 3

3. Есть коммерческая ценность и вы готовы выполнить все меры ст.10 98-ФЗ?

Да - режим КТ, сильная защита, включая увольнение, убытки, КоАП и УК. Нет - режим ИВП (информация для внутреннего пользования) с ЛНА (локальные нормативные акты), договорами, дисциплинарной и договорной ответственностью

Итог | специальный режим закона | ограничить нельзя | режим КТ | режим ИВП

Комбинируйте: КТ для ядра ценных сведений, ИВП для остальной внутренней информации, специальные режимы по закону

Режим КТ чаще всего ломается на пяти ошибках

Типовые ошибки из аудитов режимов КТ и как их исправить

Privacy Advocates

ОШИБКА	КАК ПРАВИЛЬНО
Все является КТ (коммерческая тайна), перечень на 200 пунктов	оставьте в КТ только ценное, остальное переведите в ИВП (информация для внутреннего пользования)
Нет ознакомления под подпись	ознакомьте каждого с перечнем и Положением (ст.11 98-ФЗ) и храните подписи
В перечне сведения из ст.5 98-ФЗ	сверьте перечень со ст.5, например уберите систему оплаты труда
Режим на бумаге, а папки открыты всем	разграничьте доступ и ведите учет, иначе меры не разумно достаточны (ч.5 ст.10)
NDA (соглашение о неразглашении) с контрагентом без перечня и срока	укажите состав сведений, срок конфиденциальности и неустойку

Совет эксперта: проверьте режим на одном отделе. Через месяц докажите, кто и когда получил доступ к сведениям. Не получается, значит режим только на бумаге

КТ защищает сильнее всех, но только при полном режиме

Выводы подраздела о коммерческой тайне и информации для внутреннего пользования

Privacy Advocates

1. **КТ дает самую сильную защиту**
   но только после всех пяти мер ст.10 98-ФЗ и ознакомления работников
2. **Для остальной внутренней информации**
   подходит режим ИВП на основе ст.6 149-ФЗ, ЛНА (локальные нормативные акты) и договоров
3. **Суды оценивают не названия документов**
   а реальное ограничение доступа и доказательства нарушения
4. **ИВП сохраняет регулирование и экономит ресурсы**
   действующее локальное регулирование переводится на современный правовой уровень, а набор правовых, организационных и технических мер подбирают без лишних затрат

РЕКОМЕНДАЦИЯ ЭКСПЕРТА

Держите перечень КТ коротким и конкретным

чем меньше сведений в режиме КТ, тем проще его соблюдать и защищать в суде

Практика: в деле 3 КСОЮ 2026 года Положение определяло КТ широко, но работодатель выиграл за счет ознакомления, прямого запрета и доказательств. Узкий перечень снимает и риск спора о составе КТ

36.3

Система управления ИБ

В этой части

- Правовой режим и ИБ отвечают на разные вопросы
- Систему ИБ строят в пять этапов, от обследования к контролю
- Управление ИБ - это цикл проверки и улучшения мер
- Защита строится слоями: право, организация, техника

Правовой режим и ИБ отвечают на разные вопросы

Три цели защиты информации по ст.16 149-ФЗ и связь с триадой ИБ

Privacy Advocates

Защита информации по ст.16 149-ФЗ - это **правовые, организационные и технические меры**, которые преследуют три цели

Задача ИБ

Целостность и доступность

защита от неправомерного доступа, уничтожения, изменения, блокирования, копирования и распространения

Задача правового режима

Кто вправе знать

соблюдение конфиденциальности информации ограниченного доступа

Задача ИБ

Доступность тем, кому положено

реализация права на доступ к информации

Конфиденциальность информации - обязательное требование не передавать ее третьим лицам без согласия обладателя (п.7 ст.2 149-ФЗ)

Вывод: юрист отвечает на вопрос, кто вправе знать, ИБ (информационная безопасность) - как не допустить остальных. Работает только связка

Систему ИБ строят в пять этапов, от обследования к контролю

Этапы построения системы ИБ и стандарты, на которые она опирается

Privacy Advocates

1

Обследование

инвентаризация информации, ИС (информационная система) и потоков данных, привязка массивов к режимам

2

Нормативная база

политика ИБ (информационная безопасность), Положения о КТ (коммерческая тайна) и ИВП (информация для внутреннего пользования), политика обработки ПД, правила доступа

3

Оценка рисков

модель угроз и нарушителя, оценка рисков, план их обработки

4

Внедрение мер

средства защиты, разграничение доступа, DLP (система предотвращения утечек), обучение работников

5

Контроль и улучшение

метрики, внутренний аудит, разбор инцидентов, пересмотр документов

Стандарты ГОСТ Р ИСО/МЭК 27001-2021 | ISO/IEC 27001:2022 | ГОСТ Р ИСО/МЭК 27005 для рисков | ГОСТ Р 57580.1-2017 для финансовых организаций | требования ФСТЭК для ИСПД и КИИ

Связь: защита ПД в ИСПД и СЗПД разобраны в разделе 27. Проект ФСТЭК о замене приказа № 21 не принят, срок 01.09.2026 сорван. Для госсистем с 01.03.2026 действует приказ № 117

Управление ИБ - это цикл проверки и улучшения мер

Цикл PDCA по ГОСТ Р ИСО/МЭК 27001: обеспечение ИБ это меры, управление - их цикл

Privacy Advocates

PDCA

ГОСТ Р ИСО/МЭК 27001

СУИБ

система менеджмента ИБ (информационная безопасность) повторяет цикл, пока работает организация

- обеспечение ИБ - это меры
- управление ИБ - цикл их проверки и улучшения
- результат каждого цикла - план следующего

План

Планирование

область применения, активы и их ценность, угрозы и уязвимости, оценка рисков, план обработки рисков

Делай

Внедрение

выполнение плана, внедрение мер и средств защиты, обучение и информирование работников

Проверяй

Проверка

метрики эффективности, журналы и записи, внутренний аудит, анализ инцидентов

Улучшай

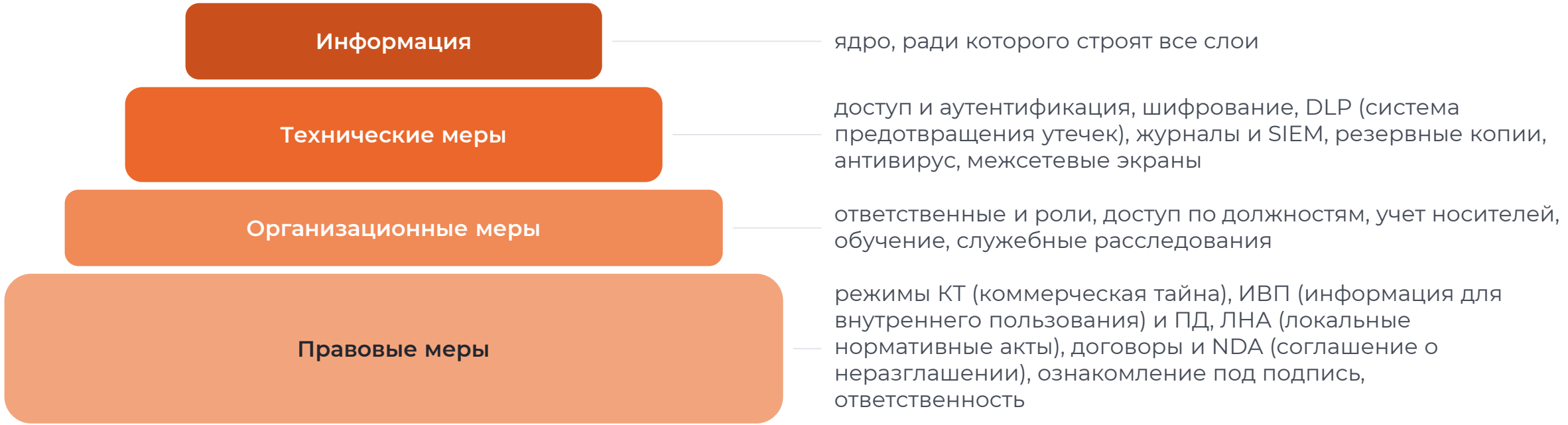
Улучшение

анализ руководства, корректирующие меры, план развития СУИБ (система управления информационной безопасностью) на следующий цикл

Защита строится слоями: право, организация, техника

Система мер защиты по ст.16 149-ФЗ вокруг защищаемой информации

Privacy Advocates



От кого защищаем | работники и бывшие работники | владельцы и топ-менеджеры | контрагенты | конкуренты | хакеры | рейдеры

Порядок: сначала правовой слой, затем техника поверх него. Технические меры исполняют режим, но правового основания конфиденциальности не создают

Без карты данных нельзя выбрать режим и настроить DLP

Выводы подраздела о системе управления ИБ

Privacy Advocates

01

Режим и ИБ (информационная безопасность) - разные вопросы

правовой режим решает, кто вправе знать, ИБ - как не допустить остальных

02

Систему строят по этапам

от обследования и нормативной базы к рискам, внедрению и контролю

03

Управление - это цикл

с метриками и аудитом, а не разовый проект

Рекомендация эксперта: первым шагом всегда идет инвентаризация информации: без карты данных нельзя выбрать режим, оценить риски и настроить DLP (система предотвращения утечек)

36.4

Мониторинг персонала и DLP

В этой части

- Контроль работников ограничен их правом на частную жизнь
- Корпоративный канал контролируют, личную переписку - нет
- DLP легализуют за шесть шагов до запуска
- Скрытый и тотальный мониторинг обесценивает доказательства

Контроль работников ограничен их правом на частную жизнь

Баланс интересов: полномочия работодателя и гарантии работника

Privacy Advocates

Работодатель вправе

- требовать исполнения обязанностей и бережного отношения к имуществу (ст.22 ТК)
- обрабатывать ПД работника для контроля качества работы и сохранности имущества (ст.86 ТК)
- контролировать соблюдение режима КТ (коммерческая тайна) (ст.10 98-ФЗ)
- определять порядок доступа к своей информации (ст.6 149-ФЗ)

vs

Работник защищен

- частная жизнь и тайна переписки (ст.23 Конституции, ст.138 УК)
- запрет собирать сведения о частной жизни и убеждениях (ст.86 ТК)
- законная цель, минимизация, биометрия только с согласия (152-ФЗ)
- право знать о контроле до его начала (ст.22, 68 ТК)

большинство

контролируют работников

по опросу 2025 года

почти половина

ведут видеонаблюдение

каждая пятая

анализирует рабочие чаты

каждая шестая

мониторит активность на компьютерах

Корпоративный канал контролируют, личную переписку - нет

Границы мониторинга: что допустимо при уведомлении работников, а что запрещено

Privacy Advocates

Формула законности: **запрет личного использования** корпоративных ресурсов, **уведомление работников**, понятная цель и минимально необходимый объем контроля

МОЖНО, ЕСЛИ РАБОТНИКИ УВЕДОМЛЕНЫ

- ✓ контролировать корпоративную почту и рабочие учетные записи
- ✓ фиксировать действия в ИС (информационная система), копирование на носители и печать
- ✓ блокировать отправку конфиденциальных файлов вовне
- ✓ вести открытое видеонаблюдение в рабочих зонах
- ✓ использовать данные DLP (система предотвращения утечек) в служебном расследовании

НЕЛЬЗЯ ИЛИ ВЫСОКИЙ РИСК

- ✗ читать личную почту и мессенджеры, даже открытые на рабочем ПК
- ✗ вести скрытое наблюдение без уведомления
- ✗ ставить камеры в зонах отдыха, раздевалках, санузлах
- ✗ идентифицировать по голосу и лицу без отдельного согласия
- ✗ мониторить личные устройства без отдельного соглашения

Практика: начальник отдела ИБ (информационная безопасность) налогового органа скопировала личные чаты сотрудников со служебных компьютеров. Приговор по ч.3 ст.272 и ч.2 ст.138 УК - 2 года условно, апелляция оставила его в силе (суд ЕАО, 31.10.2023 № 22-541/2023)

DLP легализуют за шесть шагов до запуска

Алгоритм: от целей контроля до доступа к логам

Privacy Advocates

1 **Цели и объем**

зафиксируйте цели контроля, каналы и типы данных, уберите избыточное (ч.5 ст.5 152-ФЗ). Настраивайте систему на события и метаданные, а не на сплошное содержание

2 **Запрет личного использования**

корпоративные устройства и аккаунты только для работы, закрепите это в ПВТР или ЛНА (локальные нормативные акты)

3 **Положение о мониторинге**

средства, порядок, доступ к результатам и сроки хранения (ст.8 ТК)

4 **Ознакомление**

под подпись до начала контроля. Если меняются условия труда, уведомьте за 2 месяца (ст.74 ТК)

5 **Документы по ПД**

обновите политику и перечни. Для биометрии нужно отдельное согласие (ст.9, 11 152-ФЗ), с 01.09.2025 - отдельным документом

6 **Доступ к логам**

узкий круг лиц, журнал просмотров, содержание открывают по конкретному поводу, расследование по ст.193 ТК

Результат: данные DLP (система предотвращения утечек) годятся как доказательства, а риски по ст.137 и 138 УК минимальны

Скрытый и тотальный мониторинг обесценивает доказательства

Частые ошибки при внедрении DLP и позиции регуляторов 2025 года

Privacy Advocates

СОВЕТ ЭКСПЕРТА

Сначала режимы и ЛНА (локальные нормативные акты), потом DLP (система предотвращения утечек)

система мониторинга усиливает правовой режим, но не заменяет его. Пересылку ПД на личную почту Роскомнадзор устно (27.08.2025) относит к утечке, поэтому событие оценивают как инцидент

Скрытый мониторинг, чтобы поймать нарушителя

доказательства оспоримы, есть риск ст.137 и 138 УК

Перехват личных мессенджеров и почты

тайна переписки действует и на корпоративном ноутбуке

Тотальные скриншоты и кейлоггер без цели

нарушение минимизации ПД и повод для жалоб в Роскомнадзор

Доступ к логам DLP у всех администраторов

утечка внутри системы защиты от утечек

DLP есть, а режима КТ (коммерческая тайна) нет

передача зафиксирована, но назвать ее разглашением тайны нельзя

Роструд, 26.08.2025: статистика активности ПК основанием увольнения не является: основание и проступок берут из ТК, а отчет системы остается лишь доказательством

36.5

Решение кейса и источники

- ИИ готовит проект перечня КТ, но проверяет юрист
- Решение кейса: режим вводят до инцидента, а не после
- Опорные акты и практика по защите информации

ИИ готовит проект перечня КТ, но проверяет юрист

Промпт для подготовки перечня сведений, составляющих КТ, и границы работы с моделью

Privacy Advocates

ПРОМПТ

Действуй как юрист по защите информации с опытом в ИТ-компаниях. На основе описания бизнеса **[описание без конфиденциальных деталей]** подготовь проект перечня сведений, составляющих коммерческую тайну, по ст.3 и ст.5 98-ФЗ. Сгруппируй позиции по категориям (технологии, клиенты, финансы, стратегия) и для каждой укажи, в чем ее коммерческая ценность. Отдельно перечисли сведения, которые нельзя включать в перечень по ст.5 98-ФЗ, и сведения, которые лучше защищать режимом ИВП (информация для внутреннего пользования). Не выдумывай нормы и помечай, что требует проверки юристом

ГДЕ ЗАПУСКАТЬ

- GigaChat, YandexGPT или локальная модель в контуре компании
- ИИ-агент с доступом к актуальной правовой базе, если он есть в компании

ЧТО ПРОВЕРИТЬ В ОТВЕТЕ

- ссылки только на действующие статьи
- в перечне нет сведений из ст.5 98-ФЗ
- формулировки конкретны и привязаны к бизнесу

Важно: ИИ ошибается, результат остается вашей ответственностью. Не вводите в модель ПД и сведения КТ (коммерческая тайна): суд в 2026 году учел выгрузку документов в DeepSeek при увольнении за разглашение (02-1545/2026), а замена имен не снимает ни режим ПД, ни тайну

Решение кейса: режим вводят до инцидента, а не после

Правовая оценка четырех эпизодов Альфа-Софт и что делать компании

Privacy Advocates

ЭПИЗОД	ПРАВОВАЯ ОЦЕНКА	ЧТО ДЕЛАТЬ
Разработчик ушел с кодом и базой клиентов	режим КТ (коммерческая тайна) не установлен: нет перечня, Положения и подписи. Увольнение по пп.в п.6 ч.1 ст.81 ТК и иск о разглашении КТ рискованны	защищать код как служебное произведение (ст.1295 ГК), базу - через 152-ФЗ и договор. Срочно ввести режим КТ
Архитектура и внутренние регламенты	для регламентов подходит ИВП (информация для внутреннего пользования) по ч.3 ст.6 149-ФЗ, для ядра кода и коммерческих условий - КТ	утвердить перечни КТ и ИВП, развести доступы, ознакомить работников под подпись
Финансовый директор продал облигации	использование инсайда и совет брату нарушают п.1 и 3 ч.1 ст.6 224-ФЗ, ответственность по ст.15.21 КоАП или ст.185.6 УК	проверить перечень, список инсайдеров, правила контроля и ответственное лицо, иначе компании грозит ст.15.35 КоАП
Скрытый DLP (система предотвращения утечек) читает все мессенджеры	нарушены тайна переписки и принципы 152-ФЗ, доказательства из такой системы оспоримы	пройти алгоритм легализации, отключить перехват личных каналов, ограничить скриншоты целями

Опорные акты и практика по защите информации

Нормативные акты в действующих редакциях на 10.2026 и ресурсы для самостоятельной работы

Privacy Advocates

НОРМАТИВНЫЕ АКТЫ

1. Федеральный закон от 27.07.2006 № 149-ФЗ Об информации, информационных технологиях и о защите информации
2. Федеральный закон от 29.07.2004 № 98-ФЗ О коммерческой тайне
3. Федеральный закон от 27.07.2010 № 224-ФЗ о противодействии неправомерному использованию инсайдерской информации
4. Федеральный закон от 27.07.2006 № 152-ФЗ О персональных данных
5. Указ Президента РФ от 06.03.1997 № 188 о перечне сведений конфиденциального характера
6. ГОСТ Р ИСО/МЭК 27001-2021 Системы менеджмента информационной безопасности

ПРАКТИКА И РЕСУРСЫ

Постановление КС РФ от 26.10.2017 № 25-П

пересылка служебной информации на личную почту

Определение 3 КСОЮ от 15.06.2026 № 88-10469/2026

разглашение КТ (коммерческая тайна) через личные облако и почту

Решение Бабушкинского районного суда г. Москвы от 26.05.2026 № 02-1545/2026

выгрузка документов в сервис модели при увольнении за разглашение

Банк России, противодействие инсайду

cbr.ru/inside

Telegram-канал Privacy Advocates

t.me/prv_adv

36.6

Переписка и тайна связи

- Переписку проверяют дважды: по тайне связи и по 152-ФЗ
- Два разных запрета ограничивают работу с иностранными мессенджерами
- Данные клиентов из мессенджера собирают в свою форму, а не в бот
- Запись разговора и созвона настраивают до первого звонка

Переписку проверяют дважды: по тайне связи и по 152-ФЗ

Четыре слоя сведений канала связи и почему согласие на обработку ПД не открывает доступ к сообщениям

Privacy Advocates

ЧЕТЫРЕ СЛОЯ СВЕДЕНИЙ, КАЖДЫЙ ПО СВОЕЙ НОРМЕ

1. **Идентификатор участника**
   адрес почты РКН устно считает ПД (22.07.2021-27.08.2025), изолированный номер нет (07.08.2025-14.08.2026), оба статуса спорны
2. **Метаданные обмена**
   кто, кому, когда и сколько: ПД и тайна связи, для операторов связи по ст.63 закона о связи и 345-О КС, для прочих по доктринальной позиции
3. **Содержание сообщения**
   тайна переписки (ст.23 Конституции), а ПД в части сведений о лицах, включая подписи и вложения
4. **Производные объекты**
   список участников созвона, запись и стенограмма требуют собственных основания, срока и доступа

ПЛЕНУМ ВС, 25.12.2018 № 46

Нужно согласие корреспондента

даже если личного в сообщении нет. Отсюда по экспертному подходу согласие на обработку ПД доступ к переписке не открывает

СУД И ПЕРЕПИСКА

Истребовать можно, но в объеме дела

почтовые сервисы платили штрафы по ч.9 ст.66 АПК до 100 000 ₽, а доступ к ящикам должника за пять лет суд отклонил (А53-23516/2017)

Риск: подсказки, автоответы и сортировку по содержанию писем оценивают до внедрения: разбор писем ради рекламы Мосгорсуд счел нарушением тайны (33-30344/2015), границы машинного анализа спорны

Два разных запрета ограничивают работу с иностранными мессенджерами

Ч.8 ст.10 149-ФЗ и ст.15 41-ФЗ различаются кругом лиц, действиями и перечнем, санкция - ст.13.11.2 КоАП

Privacy Advocates

ПРИЗНАК	Ч.8 СТ.10 149-ФЗ, С 01.03.2023	СТ.15 41-ФЗ, С 01.06.2025
Кого касается	названных в норме лиц при госуслугах, выполнении задания и продаже товаров, работ и услуг	шире по кругу: госорганы, Банк России, финансовые организации, операторы связи, агрегаторы, крупные соцсети, сервисы объявлений
Что запрещено	передавать платежные документы и сведения с ПД граждан РФ через системы иностранных лиц	информировать граждан РФ, по письму Минцифры от 25.06.2025 любое прямое взаимодействие, в том числе при аутентификации, кроме оказания услуг
Как узнать сервис	по перечню РКН (порядок по приказу от 21.02.2023 № 22), платформы созвонов по экспертному подходу	по признакам ч.1 ст.15, перечня нет
Ссылка без ПД	не нарушает, если информация по ссылке вне иностранной системы (письмо Минцифры 12.01.2024)	адресное сообщение со ссылкой остается информированием, канал без комментариев допустим
Пример	мировой судья 06.05.2026 (05-0478/348/2026): страховщику 100 000 ₽, нижний предел до 700 000 ₽, за одно сообщение в WhatsApp по ч.8 ст.10 и перечню	практики не найдено

Входящие: по письмам Минцифры 28.06.2023 и РКН 13.09.2023 № 08-80104, а не по норме, ПД из сервиса перечня не принимают и уничтожают, прием заявок РКН счел нарушением ч.5 ст.18

Данные клиентов из мессенджера собирают в свою форму, а не в бот

Где данные записываются впервые, кто кому обработчик и что дает национальный сервис обмена информацией

Privacy Advocates

Сбор идет мимо мессенджера

- мини-приложение: введенное сразу уходит на сервер разработчика
- встроенный просмотр страницы с формой на ресурсе оператора
- ссылка на свою форму, сама ссылка без ПД

vs

Сбор идет через мессенджер

- программный интерфейс бота: по экспертному подходу данные идут через серверы мессенджера, а боты с передачей за рубеж до записи в РФ нарушают ч.5 ст.18 (письмо РКН по обращению 22.01.2026)
- чат-бот, который запрашивает фамилию и телефон в иностранном сервисе: это сбор, а не переписка

РОЛИ ПЛАТФОРМ

- хранение данных оператора у сервиса - поручение (РКН устно, 28.01.2022-31.01.2024), примеры почты, ВКС и рассылок экспертные
- правообладатель программы в контуре оператора обработчиком не становится (РКН устно, 22.08.2025 и 27.08.2025)
- с Telegram поручения нет (письмо Управления РКН по ПФО от 19.08.2025 № 22002-8/52), по экспертному подходу и с прочими публичными

НАЦИОНАЛЬНЫЙ СЕРВИС

Добровольный канал без нового согласия

информирование по закону или договору без согласия на этот способ (ч.8 ст.1 156-ФЗ), но не реклама. Разработчик приложения и получатель сведений по инициативе пользователя - самостоятельные операторы (письмо Минцифры от 31.08.2026)

Запись разговора и созвона настраивают до первого звонка

Запрета нет: режим задают содержание, соединение и объекты сеанса, голос лишь при установлении личности

Privacy Advocates

ОБЪЕКТ	РЕЖИМ	ЧТО РЕШИТЬ ЗАРАНЕЕ
Голос	обычные ПД (РКН устно, 27.07.2023, 14.08.2026), при установлении личности спорно	при проверке по лицу или голосу письменное согласие по ч.1 ст.11 и альтернатива
Содержание беседы	частная жизнь (ст.152.2 ГК) и охраняемые тайны поверх режима ПД	о здоровье надежнее отдельные согласия на запись и передачу, РКН устно (27.08.2025) для обработчика не всегда
Номер, время, длительность	тайна связи по ст.63 закона о связи для операторов связи	для стороны разговора фактор риска по экспертному подходу
Запись, список и чат созвона	носитель с голосом и изображением всех участников	цель, информирование до начала, срок, доступ и уничтожение
Стенограмма и автопротокол	спорно	сервис расшифровки оформить поручением и назвать протокол при информировании
Основание записи	договор и интерес надежнее отзываемого согласия (экспертный подход)	без альтернативы уведомление заменяет согласие плохо, РКН устно (27.07.2023) допускал согласие продолжением разговора

ВС РФ: запрет собирать сведения о частной жизни помимо воли не касается записи участника об обязательствах сторон, если указано, когда, кем и как она сделана (33-КГ15-6, 35-КГ16-18), скрытая запись спорна

Служебный почтовый ящик часто живет дольше работника и цели

Служебная переписка, срок архива, ящик уволенного, запрос субъекта и уничтожение с журналами и копиями

Privacy Advocates

1

Ведение

письма с корпоративной почты с ФИО и названием организации идут без согласия на каждое (РКН устно, 22.10.2025), служебный чат вводят по ПВТР или ЛНА в рамках трудовой функции (Роструд, 08.09.2024)

2

Срок

по экспертному подходу срок задают каналу целиком или обосновывают долгое хранение по каждому слою переписки

3

Увольнение

спорно: срока и порядка закон не дает, конкурируют уничтожение, передача преемнику и архив на срок давности, а долго хранить без регламентации нельзя (РКН устно, 22.08.2025)

4

Уничтожение

удаленное письмо живет в резервных копиях, а перезапись журналов с ПД при продолжающейся обработке подпадает под приказ № 179 (РКН устно, 27.08.2025)

ЗАПРОС СУБЪЕКТА

Сведения об обработке, а не выгрузка ящика

ответ не включает ПД других лиц, если нет законных оснований их раскрыть (ч.2 ст.14), а письмо у второго участника оператор не удалит

ИНЦИДЕНТЫ КАНАЛА

Три сценария и три плана реагирования

открытая копия и ошибочная рассылка (уведомлять при выходе ПД наружу, РКН устно, 29.09.2022), захват учетной записи, пересылка на личную почту для работы из дома (утечка, РКН устно, 27.08.2025)

Защита информации - это режим, процессы и доказательства

Выводы раздела: карта информации, КТ и ИВП, законный мониторинг

Privacy Advocates

01

Начинайте с карты информации

чтобы понимать, какой массив к какому режиму относится

- **Рекомендация.** Проведите инвентаризацию и ведите реестр информационных активов с режимом и владельцем

02

КТ (коммерческая тайна) сильна только при всех мерах

ст.10 98-ФЗ, для остального подходит ИВП (информация для внутреннего пользования)

- **Рекомендация.** Держите перечень КТ коротким, а ИВП используйте как основной режим внутренней информации

03

Мониторинг законен при уведомлении

цели понятны, а личное отделено от рабочего

- **Рекомендация.** Внедряйте DLP (система предотвращения утечек) после ЛНА (локальные нормативные акты) и ознакомления работников, а не вместо них

Главное: защита информации - это не гриф на документе, а связка правового режима, процессов и доказательств

37

Режим коммерческой тайны

Проект по организации режима коммерческой тайны

37.1 Режимы и нарушители

37.2 Законодательство о КТ

37.3 Внедрение режима

37.4 Служебная информация

Раздел на сайте
privacy-advocates.ru/pd/ktn

37.1

Режимы и нарушители

- У компании четыре режима ограничения доступа
- Тайне угрожают свои, партнеры и противники

У компании четыре режима ограничения доступа

ПД, КТ, профессиональная тайна и ИВП доступны бизнесу, государственная и служебная тайна - органам власти

Privacy Advocates

Режимы компании

Закон или решение обладателя

- ПД - по закону для каждого оператора (152-ФЗ)
- коммерческая тайна - по решению обладателя при всех мерах 98-ФЗ
- профессиональная тайна - по закону, например банковская, врачебная, адвокатская
- ИВП (информация для внутреннего пользования) - по решению обладателя (ч.3 ст.6 149-ФЗ)

vs

Режимы государства

Только в силу закона

- государственная тайна - закон РФ О государственной тайне, работа только с лицензией и допуском
- служебная тайна - сведения органов власти с пометкой ДСП (постановление Правительства РФ № 1233)

Правило: тайну образуют три элемента закона: перечень сведений, меры ограничения доступа и ответственность. Самоназвание тайной во внутреннем документе режима не создает

Тайне угрожают свои, партнеры и противники

Потенциальные нарушители режима конфиденциальности информации компании

Privacy Advocates

Внутри

Персонал и владельцы

- работники и бывшие работники с легальным доступом
- владельцы и топ-менеджеры компании

Рядом

Контрагенты, органы власти, СМИ

- контрагенты, получившие сведения по договору
- органы власти, запросы которых исполняют только по норме закона
- средства массовой информации

Против

Конкуренты, рейдеры, преступники

- конкуренты
- рейдеры
- организованные преступные сообщества

Внутренний нарушитель: работник банка с доступом по должности сфотографировал выписку клиента и передал постороннему. Один эпизод дал два состава, ч.2 ст.183 и ч.3 ст.272 УК: легальный доступ неправомерность не снимает

37.2

Законодательство о КТ

- Режим КТ задают ГК и 98-ФЗ, технику - методики ФСТЭК
- Обладатель КТ управляет доступом и требует охраны
- Режим КТ нужен, чтобы снизить ущерб и выиграть суд
- С 2014 года ноу-хау охраняют разумными мерами, а не только КТ

Режим КТ задают ГК и 98-ФЗ, технику - методики ФСТЭК

Законодательство о коммерческой тайне: законы, указы, постановления и методические документы

Privacy Advocates

ЗАКОНЫ

1. Гражданский кодекс РФ, часть первая, от 30.11.1994 № 51-ФЗ
2. Гражданский кодекс РФ, часть четвертая, от 18.12.2006 № 230-ФЗ
3. Федеральный закон от 27.07.2006 № 149-ФЗ Об информации, информационных технологиях и о защите информации
4. Федеральный закон от 29.07.2004 № 98-ФЗ О коммерческой тайне
5. Федеральный закон от 06.12.2011 № 402-ФЗ О бухгалтерском учете

УКАЗЫ, ПОСТАНОВЛЕНИЯ, МЕТОДИКИ

- Указ Президента РФ от 06.03.1997 № 188 о перечне сведений конфиденциального характера
- постановление Правительства РСФСР от 05.12.1991 № 35 о сведениях, не составляющих КТ, утратило силу с 26.07.2025
- Методические рекомендации по технической защите информации, составляющей КТ (ФСТЭК России, 25.12.2006)
- Пособие по организации технической защиты информации, составляющей КТ (ФСТЭК России, 25.12.2006)
- СТР-К, специальные требования и рекомендации по технической защите конфиденциальной информации (приказ Гостехкомиссии России от 30.08.2002 № 282)

Учесть: методики ФСТЭК описывают техническую защиту, но режим возникает только из мер 98-ФЗ. Техника исполняет меры, а не создает их правовое основание

Обладатель КТ управляет доступом и требует охраны

Шесть прав обладателя информации, составляющей коммерческую тайну, по ст.6.1 98-ФЗ

Privacy Advocates

Обладатель КТ - лицо, которое владеет сведениями на законном основании, ограничило доступ к ним и установило режим КТ (п.4 ст.3 98-ФЗ)

- устанавливать, изменять и отменять в письменной форме режим КТ по 98-ФЗ и гражданско-правовому договору
- использовать сведения КТ для собственных нужд, не противореча законодательству
- разрешать или запрещать доступ к сведениям КТ, определять порядок и условия доступа
- требовать от получивших доступ лиц и от органов власти, которым предоставлена КТ, соблюдать обязанности по охране ее конфиденциальности
- требовать охраны конфиденциальности от лиц, получивших доступ случайно или по ошибке
- защищать свои права при разглашении, незаконном получении или использовании КТ третьими лицами, в том числе требовать возмещения убытков

Условие: обладателем КТ лицо становится только с введенным режимом. Без всех пяти мер ст.10 98-ФЗ нет ни обладателя КТ, ни этих прав

Режим КТ нужен, чтобы снизить ущерб и выиграть суд

Две цели режима по защите конфиденциальности информации

Privacy Advocates

01

ЦЕЛЬ 1

Минимизировать ущерб

от потери конфиденциальности информации

- меры разумно достаточны, если исключают доступ без согласия обладателя (ч.5 ст.10 98-ФЗ)
- короткий перечень соблюдают, широкий бизнес обходит
- ядро ценных сведений закрывают КТ (коммерческая тайна), остальное - ИВП (информация для внутреннего пользования)

02

ЦЕЛЬ 2

Защитить права в суде

взыскать убытки, уволить за разглашение, поставить вопрос об уголовной ответственности

- спор начинается с доказывания режима, а не факта раскрытия
- проверяют комплектность всех пяти мер на дату нарушения
- работает цепочка документов от перечня сведений до фиксации выгрузки

КТ не возникает сама: банковская или врачебная тайна возникают в силу закона от самой деятельности, а коммерческую тайну вводит обладатель набором мер. Без них режима нет

С 2014 года ноу-хау охраняют разумными мерами, а не только КТ

Поправки 35-ФЗ от 12.03.2014 в ст.1465 ГК и в 98-ФЗ, действуют с 01.10.2014

Privacy Advocates

До 01.10.2014

Ноу-хау только под режимом КТ (коммерческая тайна)

- секретом производства признавались сведения любого характера, в том числе о результатах интеллектуальной деятельности
- охрана возникала, только если обладатель ввел режим КТ

vs

С 01.10.2014

Ноу-хау и КТ разведены

- ноу-хау - сведения любого характера о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности (ч.1 ст.1465 ГК)
- обладатель принимает разумные меры конфиденциальности, в том числе вводит режим КТ
- ноу-хау не могут быть сведения, которые закон обязывает раскрывать или запрещает закрывать (ч.2 ст.1465 ГК)
- режим КТ применим ко всем сведениям, ценным из неизвестности третьим лицам, а не только к секретам производства

Итог поправок: обладатель секрета производства получил более широкий набор способов защиты, не ограниченный режимом КТ

Работник и бывший работник возмещают убытки от разглашения КТ

Поправки 2014 года в ст.11 98-ФЗ: кто, когда и в каких пределах отвечает

Privacy Advocates

п.3 ч.3 ст.11

Работник

возмещает убытки, если виновен в разглашении КТ (коммерческая тайна), ставшей известной ему по работе, обязательство не разглашать действует весь срок режима (п.2 ч.3 ст.11)

ч.4 ст.11

Бывший работник

отвечает так же, если разгласил сведения в течение срока действия режима КТ

ч.7 ст.11

Руководитель

возмещает организации убытки, причиненные его виновными действиями при нарушении законодательства о КТ

ч.5 ст.11

Освобождение

работник не платит, если разглашение произошло из-за несоблюдения работодателем мер режима, действий третьих лиц или непреодолимой силы

Оговорка: ст.238 ТК не дает взыскать с работника упущенную выгоду, по трудовому подходу взыщут прямой действительный ущерб, хотя и в полном размере (п.7 ч.1 ст.243 ТК). Включают ли убытки по ст.11 98-ФЗ упущенную выгоду, вопрос спорный

КТ делится на ноу-хау и деловую информацию

Два вида сведений под режимом КТ: исключительное право на секрет производства и деловая информация

Privacy Advocates

ПРИЗНАК	СЕКРЕТ ПРОИЗВОДСТВА (НОУ-ХАУ)	ДЕЛОВАЯ ИНФОРМАЦИЯ
Что охраняет	сведения любого характера о результатах интеллектуальной деятельности в научно-технической сфере и о способах профессиональной деятельности	иные сведения, ценные из неизвестности третьим лицам
Пример	технологии, чертежи, исходный код, рецептуры	клиентская база, условия сделок, себестоимость, стратегия
Норма	ст.1465-1472 ГК, 98-ФЗ	ст.3 и 10 98-ФЗ
Способ охраны	исключительное право, пока сохраняется конфиденциальность (ст.1467 ГК), разумные меры, в том числе режим КТ (коммерческая тайна)	**только режим КТ со всеми мерами ст.10**
При нарушении	возмещение убытков по ст.1472 ГК и ответственность за разглашение КТ	дисциплинарная, гражданско-правовая, административная и уголовная по ст.14 98-ФЗ

Связка: исключительное право на ноу-хау живет, пока сведения конфиденциальны. Раскрытие прекращает и право, и режим КТ, поэтому ноу-хау держат в перечне КТ

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
ZIN-009	КТ возникает только при четырех признаках одновременно	36 Защита информации
ZIN-010	Сведения из ст.5 98-ФЗ не станут КТ даже с грифом	36 Защита информации

37.3

Внедрение режима

- Пакет режима КТ: три приказа, Положение и шесть форм
- Режим КТ внедряют в четыре этапа, от аудита до грифа
- Контроль режима КТ идет от перечня к мерам
- Подсистема ИБ исполняет режим КТ, но не заменяет его

Пакет режима КТ: три приказа, Положение и шесть форм

Комплекс локальных актов в сфере коммерческой тайны

Privacy Advocates

ПРИКАЗЫ

1. об утверждении Положения о режиме КТ и назначении ответственного за организацию режима
2. об утверждении перечня подразделений и должностей с правом доступа к КТ
3. об утверждении перечня сведений, составляющих КТ

ЦЕНТР ПАКЕТА

Положение о режиме КТ

порядок обращения со сведениями, доступ, учет, гриф, контроль и ответственность

- утверждается первым приказом
- с ним знакомят под подпись (ст.11 98-ФЗ)

ТИПОВЫЕ ФОРМЫ

- соглашение о неразглашении
- журнал учета материальных носителей
- журнал учета лиц, получивших доступ
- журнал учета лиц, которым сведения предоставлены или переданы
- акт передачи материальных носителей
- акт уничтожения материальных носителей

Экспертная группировка: минимум режима укладывается в три документа: Положение о порядке обращения, перечень сведений и соглашения о конфиденциальности с работниками и контрагентами. Комплектность проверяют по их согласованности и исполнению всех пяти мер

Режим КТ внедряют в четыре этапа, от аудита до грифа

Проект по организации режима коммерческой тайны

Privacy Advocates

1

Исследование

внутренние документы, системы и подразделения компании, связанные с оборотом сведений КТ

2

Границы режима

перечень категорий сведений КТ, перечень систем с ними и перечень категорий лиц, которым сведения предоставляются или передаются

3

Регламентирование

правила обработки и защиты сведений КТ в локальных актах, трудовых договорах с работниками и договорах с контрагентами

4

Привязка и гриф

сопоставление категорий КТ с документами и базами данных, определение работников с доступом, нанесение грифа на носители

Результат этапов

- карта оборота сведений КТ
- перечни сведений, систем и получателей
- ЛНА (локальные нормативные акты), трудовые договоры и NDA (соглашение о неразглашении)
- учет допущенных и гриф на носителях

Итог проекта: режим конфиденциальности информации дает судебную защиту. Без завершенного проекта спор об убытках или увольнении часто проигрывается на отсутствии режима, а не на существе нарушения

Контроль режима КТ идет от перечня к мерам

Как сведения компании становятся КТ и чем обеспечивается их конфиденциальность

Privacy Advocates

ШАГ 1

Сведения

технологии, клиенты, финансы и планы компании

ШАГ 2

Отнесение к КТ

перечень КТ (коммерческая тайна) выделяет из сведений то, что отвечает признакам ст.3 98-ФЗ

ШАГ 3. МЕРЫ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ КТ

Гриф КТ
на носителях и в реквизитах документов, с наименованием и местом нахождения обладателя

Контроль доступа
порядок обращения со сведениями и контроль его соблюдения

Допущенные сотрудники
учет лиц, получивших доступ, и лиц, которым сведения переданы

Ознакомление с правилами
под подпись с перечнем, режимом и ответственностью (ст.11)

Меры защиты, DLP
технические меры по ч.4 ст.10, учитываются при оценке разумной достаточности

Контроль: первым в споре проверяют комплектность мер на дату нарушения, поэтому даты актов, расписок и нанесения грифа фиксируют документально

Подсистема ИБ исполняет режим КТ, но не заменяет его

Технические функции, которые поддерживают режим КТ в информационных системах

Privacy Advocates

Защищенные области

отдельные хранилища для сведений КТ (коммерческая тайна)

Многофакторная аутентификация

вход к сведениям КТ по нескольким факторам

Разграничение полномочий

доступ по должностям из перечня

Ограничение доступа к документам

права на чтение, копирование и печать

Динамическая настройка правил

правила меняются вместе с перечнем и составом допущенных

Постоянный аудит

журналы обращений к сведениям КТ

Формирование отчетов

для ответственного за режим и служебных расследований

Порядок внедрения

сначала Положение, перечень и NDA (соглашение о неразглашении), затем техника. Гриф проставляют автоматически в шаблонах и выгрузках

DLP контролирует каналы утечки, от почты до буфера обмена

Data Loss/Leak Prevention: технологии и устройства предотвращения утечек из ИС вовне

Privacy Advocates

ОПРЕДЕЛЕНИЕ

DLP

технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также программные или программно-аппаратные устройства для такого предотвращения

КАНАЛЫ СВЯЗИ

- почта на шлюзе
- HTTP-трафик
- мессенджеры
- IP-телефония
- социальные сети
- поисковые запросы
- P2P-сети
- FTP

УСТРОЙСТВА И РАБОЧИЕ МЕСТА

- съемные носители
- печать и сканирование
- беспроводные сети
- буфер обмена
- сканирование рабочих станций

ХРАНИЛИЩА И ИНТЕГРАЦИИ

- базы данных и сетевые хранилища
- архивы и документы
- интеграция с СЭД, LDAP и прокси
- работа в виртуальной среде



Настройка: система фиксирует события, содержание открывают по сработавшему правилу. Легализация DLP - в разделе 36

За разглашение КТ отвечают по ГК, ТК, КоАП и УК

Ст.14 98-ФЗ: дисциплинарная, гражданско-правовая, административная и уголовная ответственность

Privacy Advocates

ГК, ТК И КОАП

ст.15 ГК
убытки обладателю охраняемой законом тайны

ст.1472 ГК
убытки за неправомерное использование или разглашение ноу-хау, если иное не предусмотрено законом или договором

пп.в п.6 ч.1 ст.81 ТК
увольнение за разглашение охраняемой законом тайны, ставшей известной по работе

п.7 ч.1 ст.243 ТК
полная материальная ответственность работника за разглашение охраняемой законом тайны

ст.13.14 КоАП
разглашение информации ограниченного по закону доступа лицом, получившим ее по службе: должностному лицу 40-50 тыс. ₽ или дисквалификация до 3 лет, юрлицу 100-200 тыс. ₽

СТ.183 УК

ЧАСТЬ	ДЕЯНИЕ	НАКАЗАНИЕ
ч.1	собирание сведений КТ (коммерческая тайна) похищением документов, подкупом, угрозами или иным незаконным способом	до 2 лет лишения свободы, штраф
ч.2	разглашение или использование КТ без согласия владельца лицом, которому она доверена или известна по работе	до 3 лет, штраф до 1 млн ₽, запрет занимать должности
ч.3	те же деяния с крупным ущербом или из корыстной заинтересованности	от 2 до 5 лет лишения свободы, штраф до 5 млн ₽
ч.4	деяния ч.2 или 3, повлекшие тяжкие последствия	**от 3 до 7 лет**

37.4

Служебная информация

- Режимы КТ, ИВП и ПД пересекаются и складывают ограничения
- Режим ИВП закрывает то, что КТ и ПД не охватывают

Режимы КТ, ИВП и ПД пересекаются и складывают ограничения

Как соотносятся коммерческая тайна, служебная информация и ПД в одной компании

Privacy Advocates

КТ и ПД

Действуют оба режима

клиентская база с данными граждан закрыта КТ и защищена 152-ФЗ. КТ не расширяет полномочий по ПД и не заменяет основания обработки

ИВП и ПД

ИВП не заменяет 152-ФЗ

регламенты и кадровые материалы с ПД работников остаются под режимом ПД, внутренний режим не может быть либеральнее закона

КТ и ИВП

Ценное в КТ, остальное в ИВП (информация для внутреннего пользования)

чувствительное, но не ценное из неизвестности выводят во внутренний режим, и перечень КТ разгружается

Инструмент: карту режимов ведут по категориям сведений, а не по документам: для каждой категории указывают, ПД ли это и какая тайна на нее наложена

Режим ИВП закрывает то, что КТ и ПД не охватывают

Особенности и преимущества внутреннего режима конфиденциальности компании

Privacy Advocates

01

Преемственность

локальное регулирование сохраняется и переводится на современный правовой уровень

02

Системный подход

сферы регулирования разграничены с действующими режимами ПД и КТ (коммерческая тайна)

03

Экономия

оптимальный набор правовых, организационных и технических мер решает задачи без лишних затрат

04

Контрагенты

отношения урегулированы там, где режимы КТ и ПД невозможны или избыточны

Цена режима: ИВП (информация для внутреннего пользования) не дает защиты профильного закона и уголовной нормы, но и не требует полного набора мер. Нарушение при надлежащем ознакомлении - основание дисциплинарной ответственности

Эта тема раскрыта в других разделах

Слайды живут в одном месте Альманаха, клик по строке открывает слайд в его разделе

Privacy Advocates

СЛАЙД	ЗАГОЛОВОК	РАЗДЕЛ
ZIN-014	ИВП закрывает внутреннюю информацию без строгости КТ	36 Защита информации

ФИНАЛ

Ресурсы и контакты

Чек-лист, дайджест и контакты Privacy Advocates

Чек-лист из основных контролей обработки и защиты ПД

Контроли комплаенса ПД в 10 разделах с мерами ответственности и риск-факторами

Privacy Advocates

	РАЗДЕЛ	КОНТРОЛЕЙ	САНКЦИИ
01	Руководство и учет в области ПД	10	⚡
02	Целенаправленность и пропорциональность	9	⚡
03	Основания обработки ПД	26	⚡⚡
04	Сбор, использование, хранение и уничтожение ПД	17	⚡⚡⚡
05	Передача ПД и соглашения с третьими лицами	15	⚡⚡
06	Взаимодействие с субъектами ПД	18	⚡
07	Взаимодействие с уполномоченными органами	11	⚡
08	Осведомленность и обучение персонала	4	⚡
09	Безопасность обработки ПД	15	⚡⚡⚡
10	Контроль отклонений и реагирование на инциденты	7	⚡⚡

132 контроля: нормы, ссылки, санкции и риск-факторы по каждому

Чек-лист обработки и защиты ПД

Скачать с Яндекс Диска

Прил. 1 меры ответственности **Прил. 2** риск-факторы проверок **Прил. 3** сокращения

Дайджест значимых событий и инициатив в области ПД

Регулярно обновляемый свод законов, проектов, практики и повестки

Privacy Advocates

ЧТО ВНУТРИ

Федеральные законы, акты Президента и Правительства, ведомственные акты и проекты с датами вступления в силу.

Правоприменительная практика судов, РКН, ФАС и прокуратуры с реквизитами и тезисами.

Инициативы, события и аналитика регуляторов, депутатов, экспертного сообщества и рынка.

Метка актуальности и отметки New у поступлений последнего периода.



Дайджест 2026

privacy-advocates.ru/pd/dst

Альманах Privacy Advocates

Шаблоны, чек-листы и калькуляторы

Рабочие инструменты DPO: открываются по клику и по QR, файлы лежат на Яндекс Диске

Privacy Advocates

05 Калькулятор индекса атрибутивности
раздел Определение ПД

06 Проект Положения об обработке и защите ПД
раздел Допустимость

07 Чек-лист обработки и защиты ПД
раздел Организация

07 Типовая форма реестра обработки (RoPA)
раздел Организация

10 Калькулятор применимости законного интереса
раздел Основания

15 Биометрия в СКУД, аналитическая записка
раздел Биометрия

19 Калькулятор стратегий локализации
раздел Локализация

21 Шаблон соглашения о поручении (DPA)
раздел Поручение и DTA

21 Шаблон соглашения о передаче ПД (DTA)
раздел Поручение и DTA

21 Data Transfer Addendum для ГПХ и NDA
раздел Поручение и DTA

21 Чек-лист оценки третьих лиц
раздел Поручение и DTA

24 Чек-лист перед запуском ИИ
раздел ИИ и ПД

26 Калькулятор рисков обработки ПД
раздел Прайваси-риски

26 Пособие к калькулятору рисков
раздел Прайваси-риски

29 План профвизитов Роскомнадзора на 2026 год
раздел РКН и органы

29 Перечень материалов Роскомнадзора
раздел РКН и органы

Схемы и статьи

Схемы регулирования и статьи Privacy Advocates, файлы лежат на Яндекс Диске

Privacy Advocates

03 Комментарий к 266-ФЗ
раздел Обзор комплаенса

05 Квантовая механика инфоприватности
раздел Определение ПД

10 Схема свойств согласия
раздел Основания

10 Схема модели получения согласия
раздел Основания

10 Схемы фильтрации законного интереса
раздел Основания

13 Схема регулирования массовых вызовов
раздел Маркетинг

14 ПД в литературных произведениях
раздел Распространение

15 Сценарии обработки биометрических ПД
раздел Биометрия

18 Схема требований и методов обезличивания
раздел Уничтожение ПД

21 Соглашения о поручении и передаче ПД
раздел Поручение и DTA

22 Схема рекомендательных технологий
раздел Сайт

26 Схема риск-менеджмента ПД
раздел Прайваси-риски

26 Вред информационной приватности
раздел Прайваси-риски

27 Анализ ПП № 1119
раздел Защита и СЗПД

30 Расчет оборотных штрафов
раздел Ответственность

36 Почта, мессенджеры и ВКС
раздел Защита информации

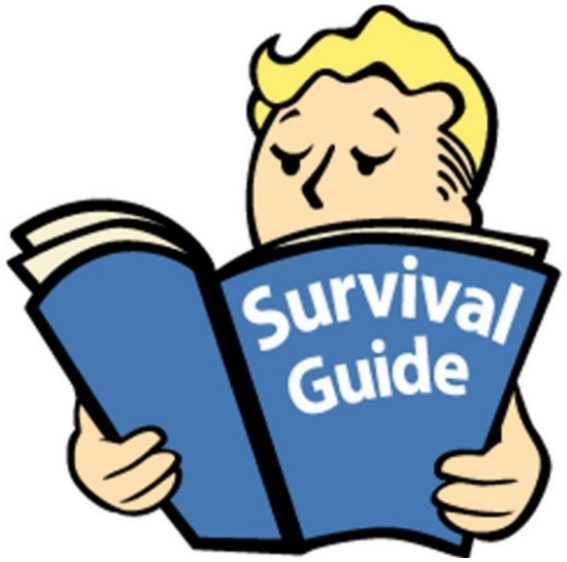
ФИНАЛ

Юмор Альманаха

Карикатуры о персональных данных и информационной приватности

Privacy Advocates

**В прайваси комплаенсе у вас не бывает проблем,
у вас бывают приключения.**



Privacy Advocates

Если вы провалили задание в прайваси комплаенсе, то оно просто становится другим заданием.

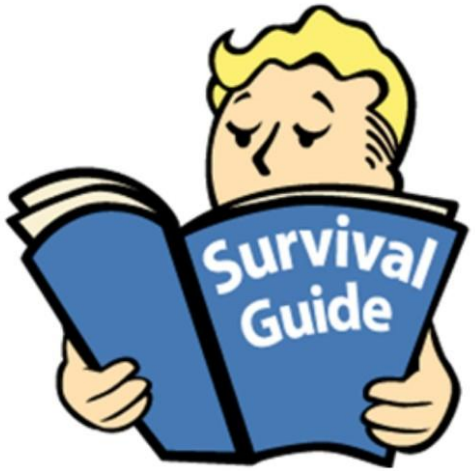


Privacy Advocates

Никаких персональных данных в окружающем человека мире нет.

Есть только активность человеческого ума по их поводу.





Комплаенс ПД – это BDSM, а ты не знаешь «стоп-слово»

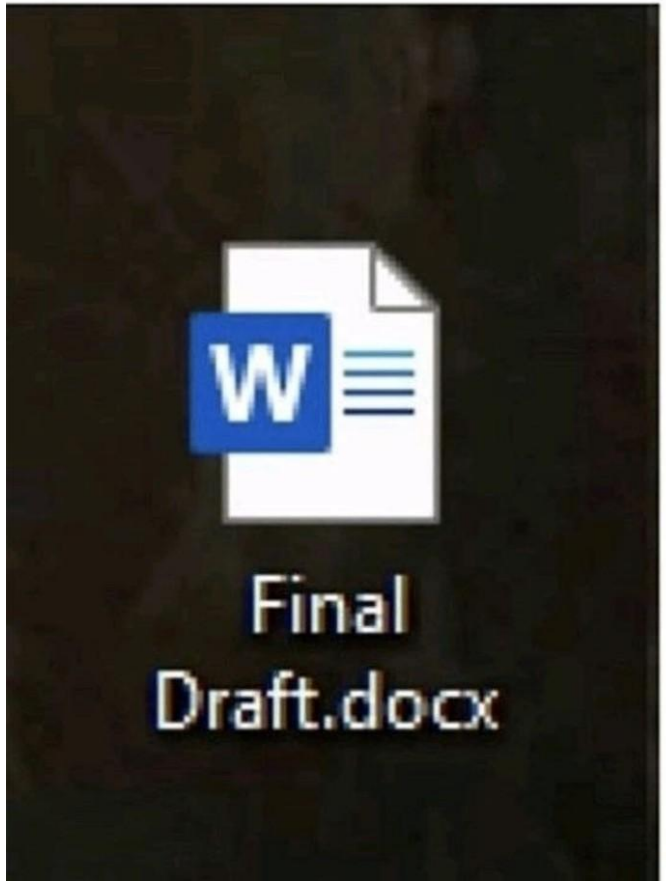
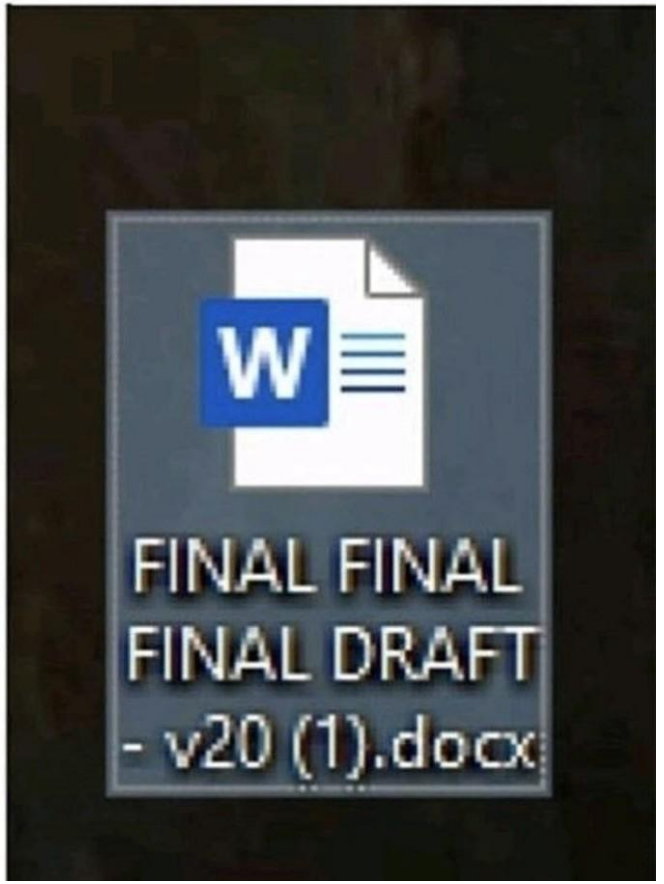
*BDSM - Business, Development, Sales & Marketing

Privacy Advocates



Privacy Advocates

Когда разрабатываешь Политику конфиденциальности...

чем все закончилось	*чем все закончилось на самом деле*
	

Юмор Альманаха ПД



Privacy Advocates



Юмор Альманаха ПД



Privacy Advocates

Когда ~~прилег постоять сидя~~ используешь несколько правовых оснований для одной и той же обработки персональных данных



Privacy Advocates

Пять стадий принятия неизбежного: комплаенс ПД



Отрицание	Гнев	Торговля	Депрессия	Принятие
Штраф – всего лишь 100 тысяч рублей!	Не трогайте бизнес-процессы!	А разве ПД есть где-то, кроме HR?	Почти все обрабатывают ПД...	Ну, хорошо, давайте проведем аудит

Privacy Advocates

Чем хороша профессия прайвасиста



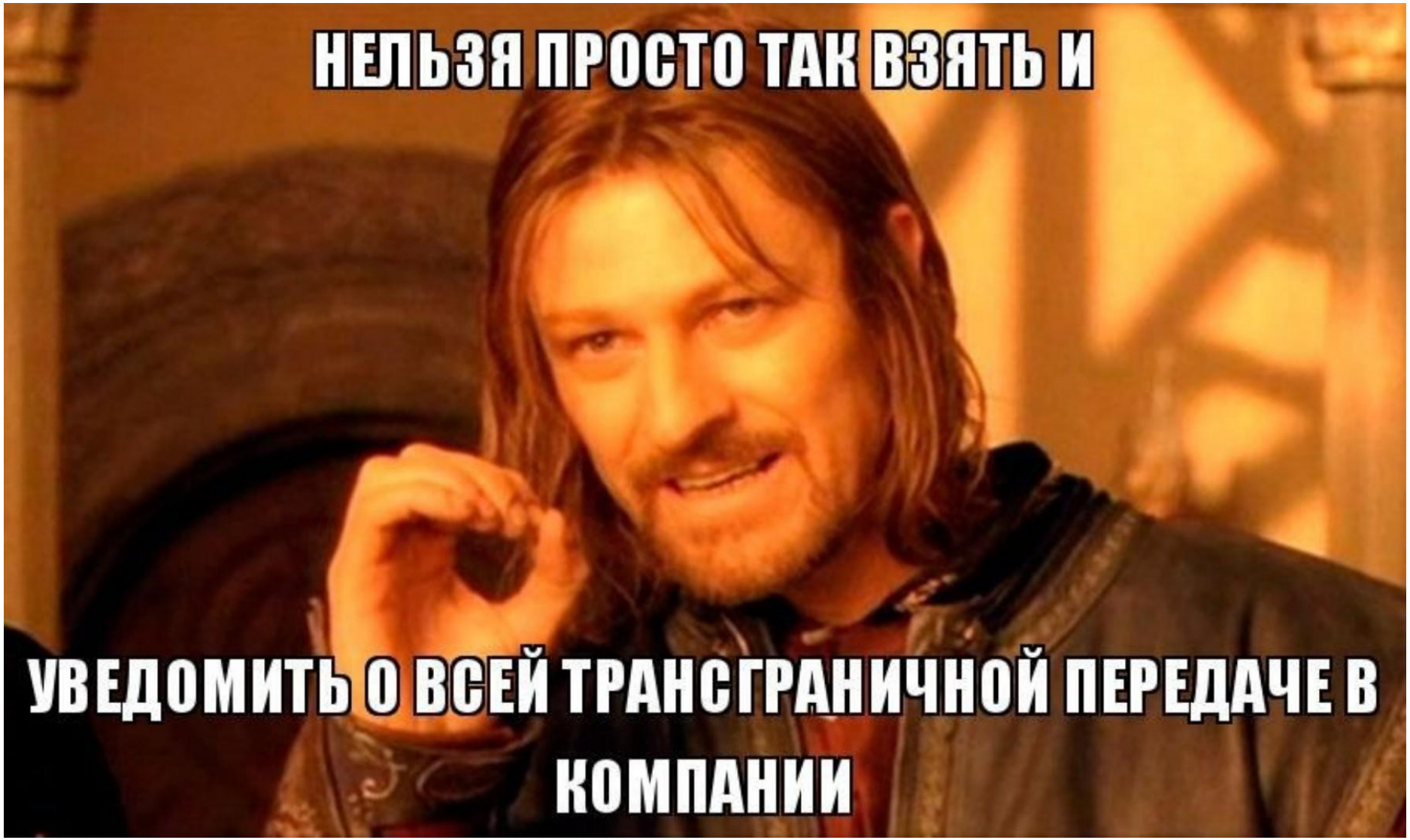
Privacy Advocates



Privacy Advocates

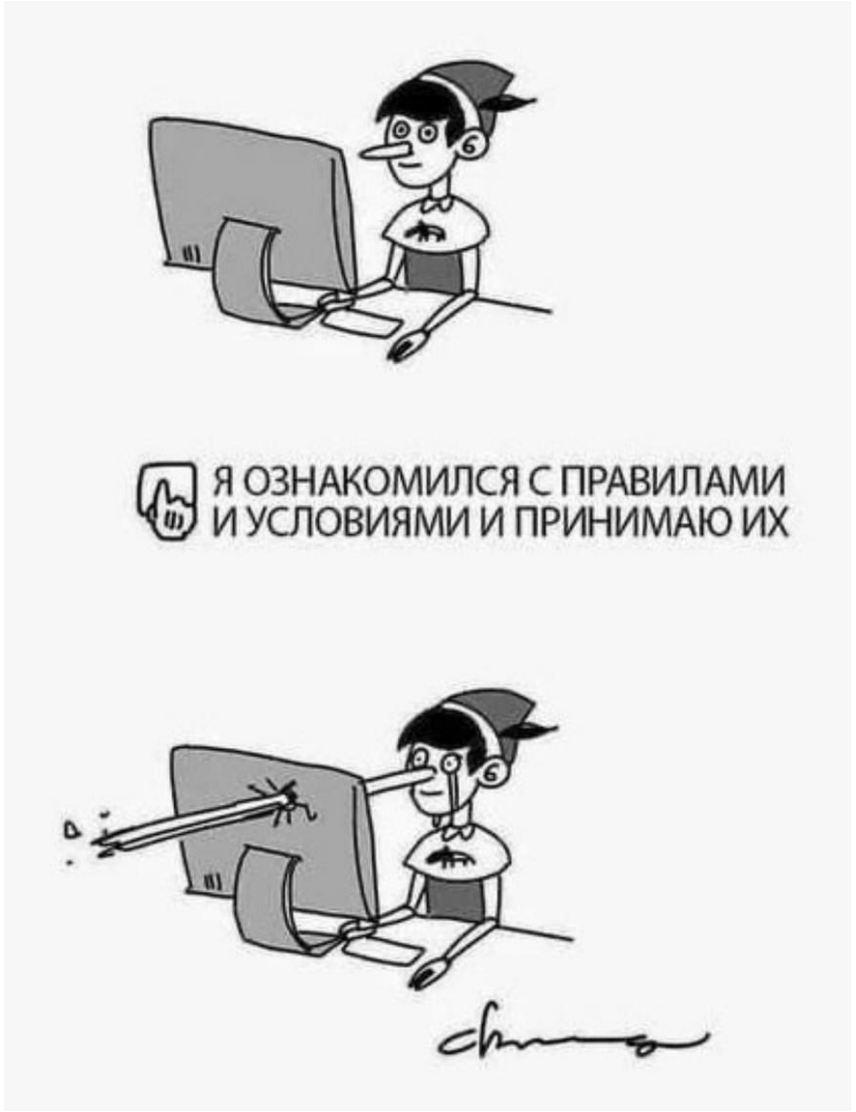
Быть DPO:
20% - вдохновение
30% - пот, слезы и бессонница
50% - выравнивание строчек документа в Word

Privacy Advocates




Оптимист
Стакан наполовину полон
Пессимист
Стакан наполовину пуст
Начинающий DPO
Вода занимает половину объёма стакана
Матёрый DPO
Стакан в два раза больше, чем должен быть

Юмор Альманаха ПД



Privacy Advocates

DPO раньше



- Стал ~~суперменом~~ DPO поневоле
- Учился в ходе проверок РКН
- Читал комментарий Приезжевой к 152-ФЗ
- Выменивал тексты предписаний РКН у других DPO
- Подписан на Лукацкого и Емельянникова
- Лично локализовал базы с ПД за час до проверки РКН
- Моделировал угрозы безопасности ПД

DPO сейчас



- Развивает личный бренд
- Учится на курсах RPPA и Б152
- Читает комментарий Савельева к 152-ФЗ
- Конспектирует вебинары РКН
- Подписан на Горелкина и ПЕРСОНЕМЫ
- Прокачивает софт скиллз
- Ведет свой ТГ-канал

Privacy Advocates



Privacy Advocates



Девопс не просто умное слово, но ещё и очень быстрое дело. Пока хакеры планируют вектора атаки, мы меняем архитектуру - причём без документации.
Когда приходит время взлома, хакер теряется на незнакомом облаке и приходит в полную небоеготовность. Так мы закрываем все уязвимости.




МЕНЯ ИНОГДА ПОСЕЩАЮТ ОЧЕНЬ МРАЧНЫЕ МЫСЛИ, КИСА...
...С КОТОРЫМИ Я МОГУ ПОДЕЛИТЬСЯ ТОЛЬКО С ТОБОЙ.
ВОТ К ПРИМЕРУ...
Рассказывает о будущих штрафах за утечки ПД...
ХОТЯ, ЗНАЕШЬ, НАВЕРНОЕ, ОНИ НЕ ТАКИЕ УЖ И МРАЧНЫЕ, В КОНЦЕ КОНЦОВ.
/jimbentonshots

Privacy Advocates

Люди делятся на две категории:
на тех, кто читает законодательство о ПД,
и тех, кто слушает тех, кто читает.

Privacy Advocates

DPO нужно уметь появляться в ненужном месте в ненужное время, чтобы узнавать нужную информацию.

Privacy Advocates

Когда вслух говоришь о желании купить какую-то вещь рядом со смартфоном

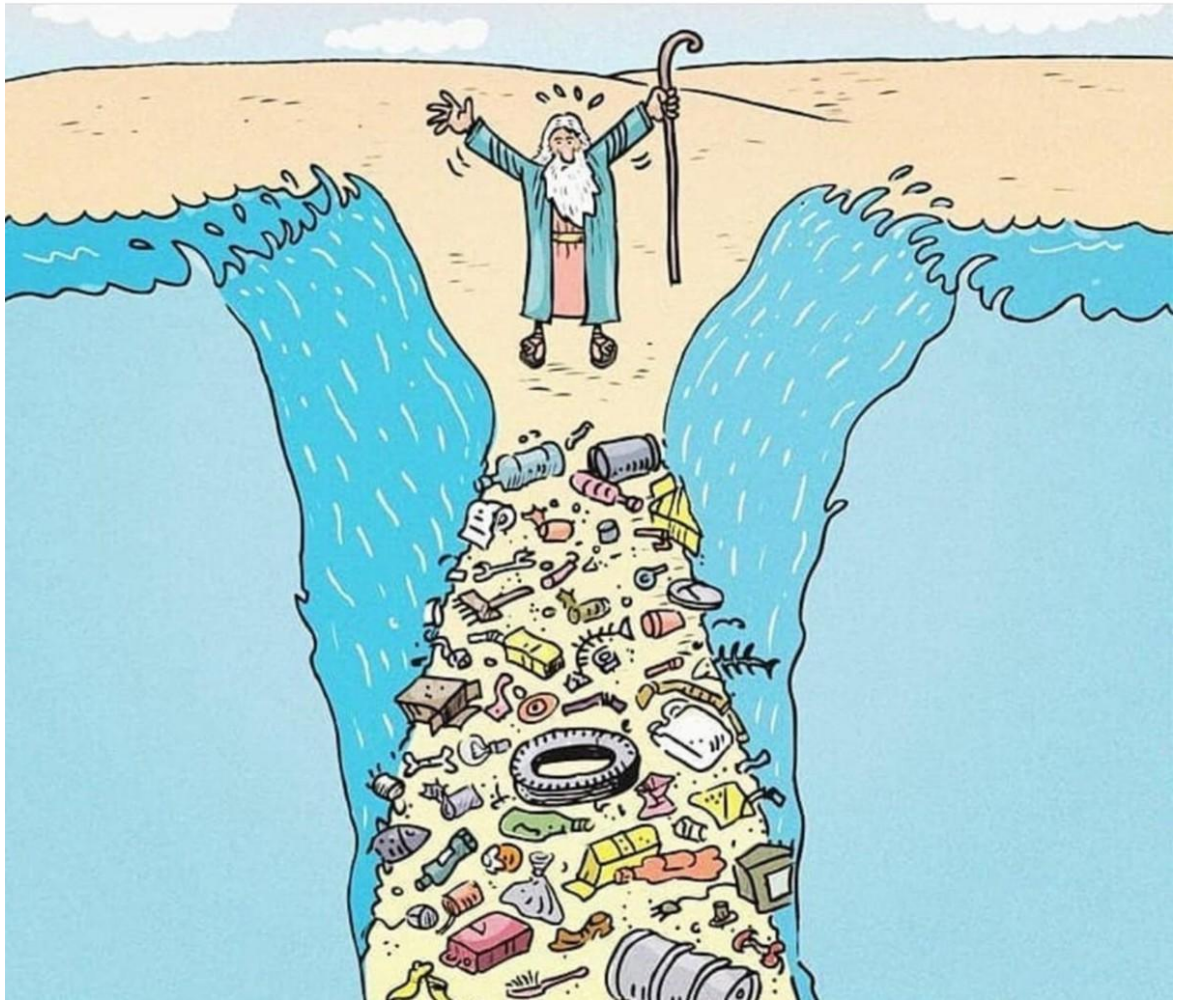


Privacy Advocates



Privacy Advocates

Типичный анализ процесса обработки ПД



Privacy Advocates

Художник: «Я так вижу»

Актёр: «Я так чувствую»

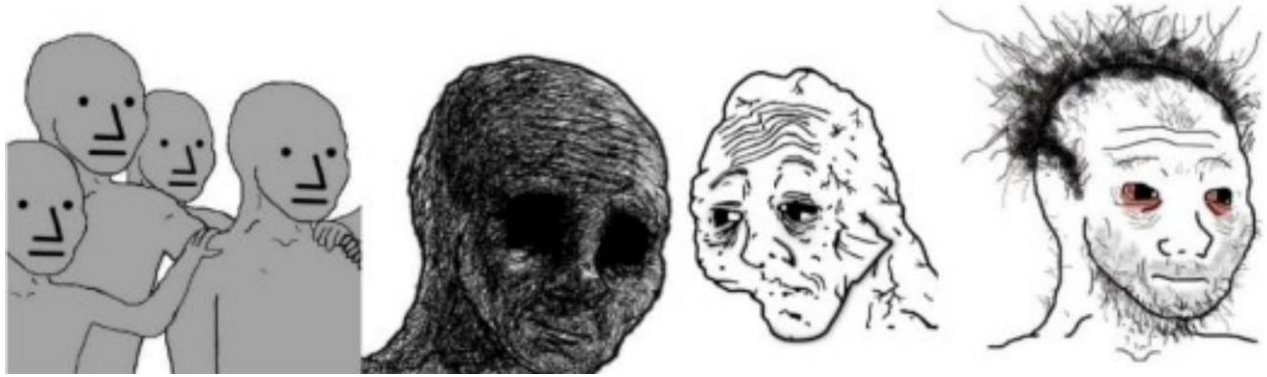
DPO: «Я так больше не могу»

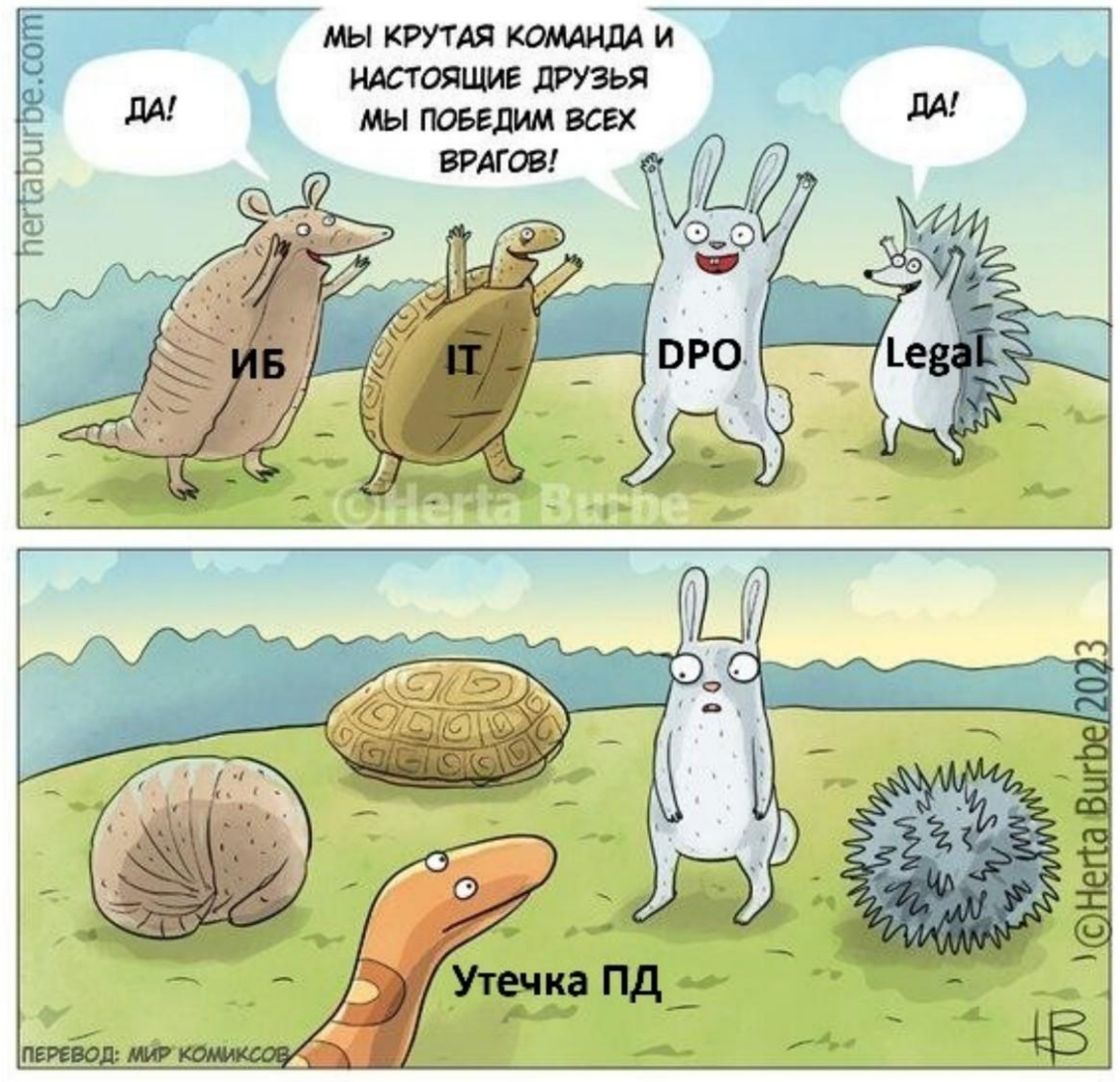
Privacy Advocates

Те, кто изучают чужие согласия на обработку персональных данных



Те, кто создают эти согласия




hertaburbe.com
ДА!
МЫ КРУТАЯ КОМАНДА И НАСТОЯЩИЕ ДРУЗЬЯ МЫ ПОБЕДИМ ВСЕХ ВРАГОВ!
ДА!
ИБ
IT
DPO
Legal
©Herta Burbe
Утечка ПД
ПЕРЕВОД: МИР КОМИКСОВ
©Herta Burbe 2023

Privacy Advocates

Желание стать крутым DPO и защищать права людей при обработке их данных



Желание взаимодействовать с людьми



Privacy Advocates



Privacy Advocates

Краткий определитель privacy документов по жанрам:

1) красиво, приятно, дорого - политика;

2) длинно, умно, непонятно - положение;

3) скучно, страшно, сложно - согласие;

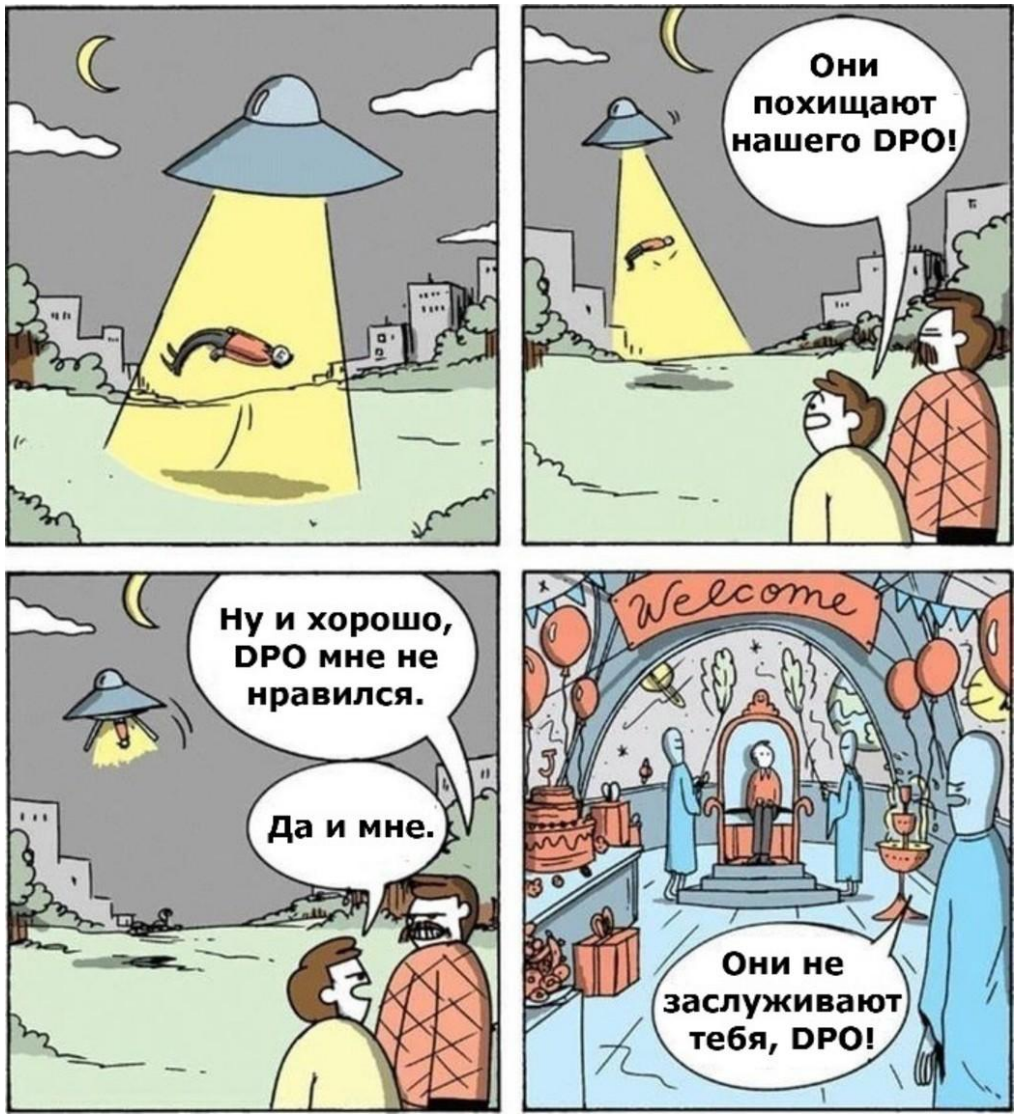
4) кратко, чётко, императивно - запрос от РКН.


Вот такая вот идея!
Что скажете?
Хитрый консалтинг
Договор
Согласие
Обработчик
Оператор
proidemtes

Privacy Advocates

Если хотите узнать, как работает голова DPO, представьте себе веб-браузер с открытыми 2879 вкладками. Работающими. Всё. Время.




Они похищают нашего DPO!
Ну и хорошо, DPO мне не нравился.
Да и мне.
Welcome
Они не заслуживают тебя, DPO!

Privacy Advocates



Privacy Advocates

Ответственность за нарушения в области персональных данных как сказка – *чем дальше, тем страшнее*



Privacy Advocates

КАК DPO ЗАВАРИВАЮТ ЧАЙ



Privacy Advocates



Privacy Advocates

Оператор оплачивает оборотный штраф за утечку



Privacy Advocates

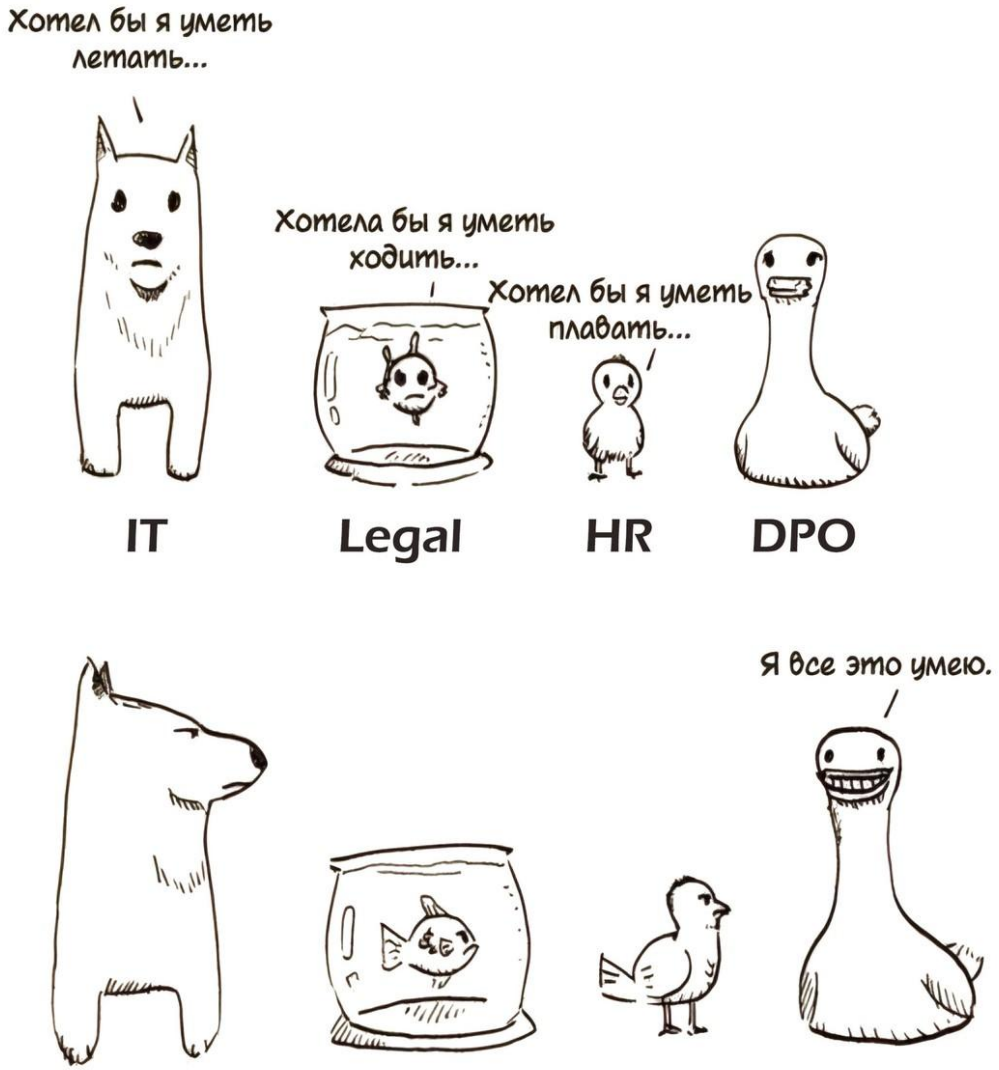
Ты одинок? Тебя все игнорируют? Никто тебе не звонит и никуда не зовёт? Выучись на DPO! Ты будешь нужен всем и каждому - в любое время дня и ночи!

Privacy Advocates

Будни прайвасиста:

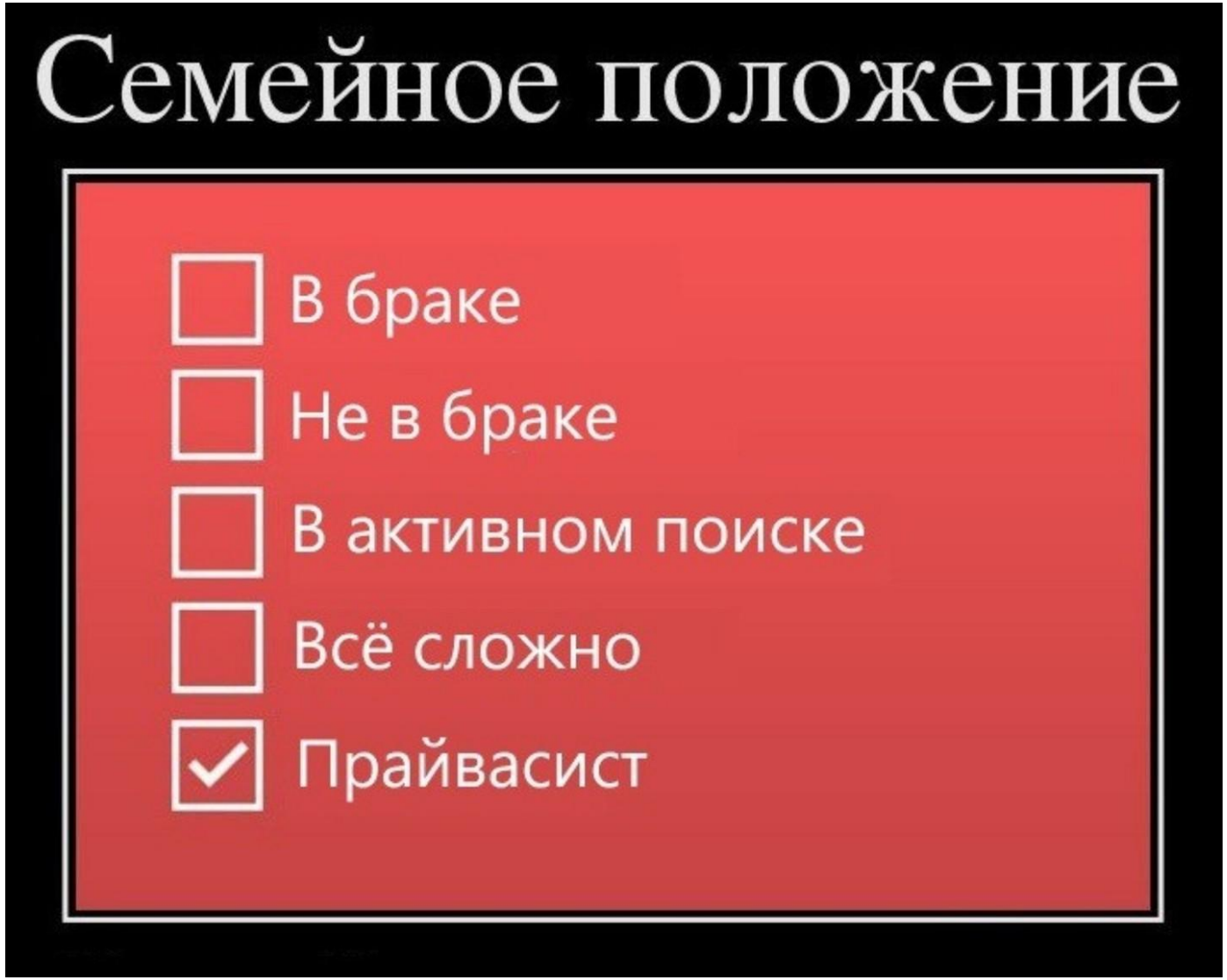


**ТОТ, КОГО ВИЖУ ЧАЩЕ,
ЧЕМ РОДНЫХ**


Хотел бы я уметь летать...
Хотела бы я уметь ходить...
Хотел бы я уметь плавать...
IT
Legal
HR
DPO
Я все это умею.

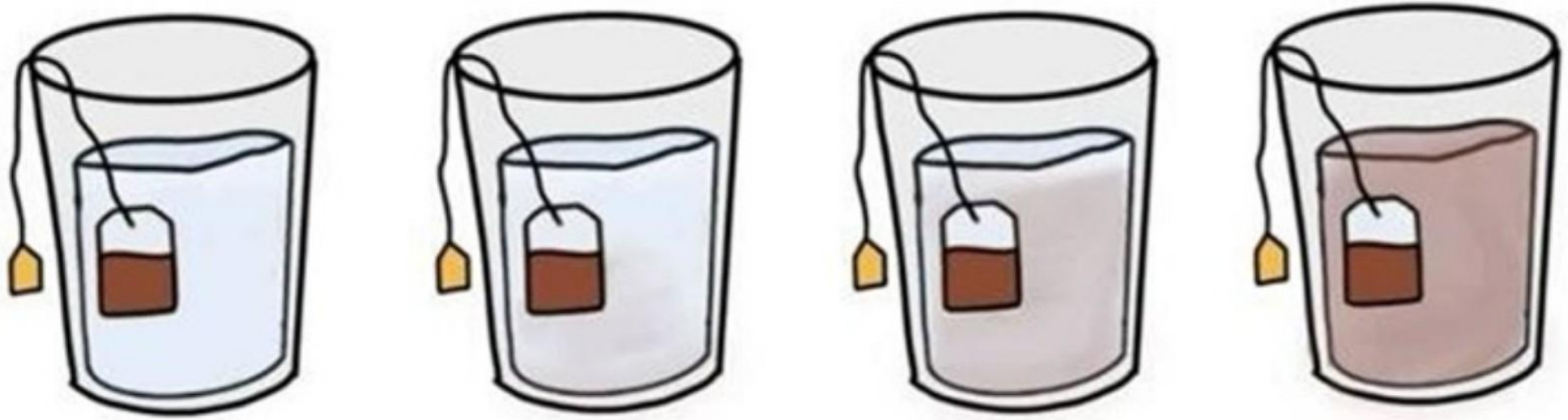

Да поймите же вы, наконец, что это просто реклама очередного privacy-обучения. В настоящей жизни такой уровень privacy-комплаенса недостижим.
©DAN PIKARO. 3.2.12
Dist. by King Features
BIZARROCOMICS.COM

Privacy Advocates



Privacy Advocates

ПРИ ВНЕДРЕНИИ КУЛЬТУРЫ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ ИНОГДА ВСЁ, ЧТО НУЖНО СДЕЛАТЬ, ЭТО ТЕРПЕЛИВО ЖДАТЬ



- Как работа DPO?
- Норм... Очень... Много... Норм...



Privacy Advocates




DPO
DPO
Понятное и предсказуемое регулирование ПД
DPO


Улиточка, мы получили запрос на доступ к ПД! Ответь на него как можно скорей!
Улиточка, мы не смогли идентифицировать субъекта, направившего нам запрос! Не отвечай на него!!!
DPO месяца



«Пусть я выгляжу как утка и крякаю как утка – внутри меня бьется сердце ответственного за организацию обработки ПД!»

Юмор Альманаха ПД




Стой! Тут где-то сидят "разбирающиеся в ПД"...
Как узаконить обработку ПД?
Возьми согласие
Уведоми РКН
Опубликуй политику

Юмор Альманаха ПД



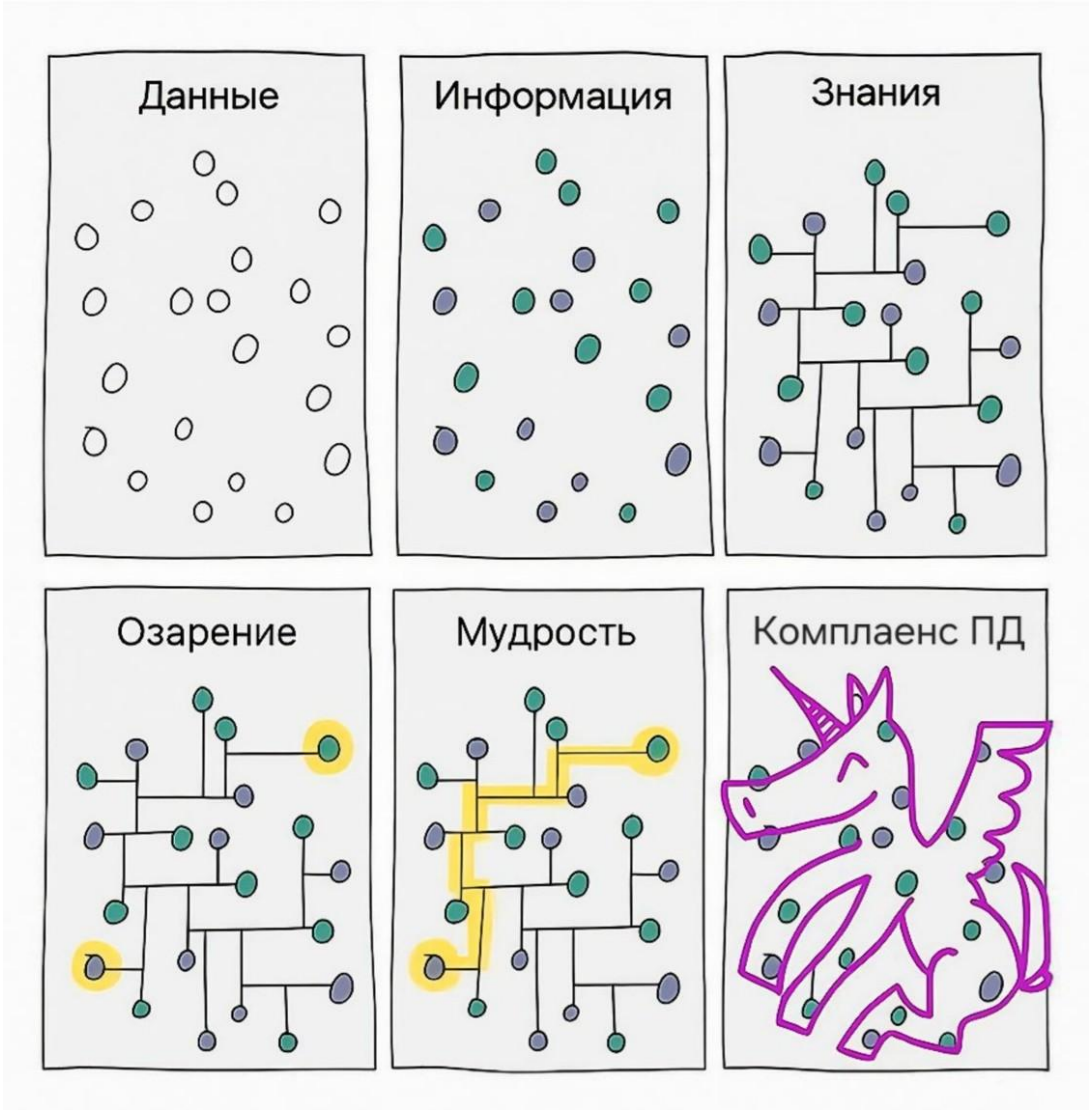
Я ПРИНИМАЮ COOKIES НА КАЖДОМ САЙТЕ, НА КОТОРЫЙ ЗАХОЖУ, ПОНЯТИЯ НЕ ИМЕЯ, ЧТО ЭТО ТАКОЕ:



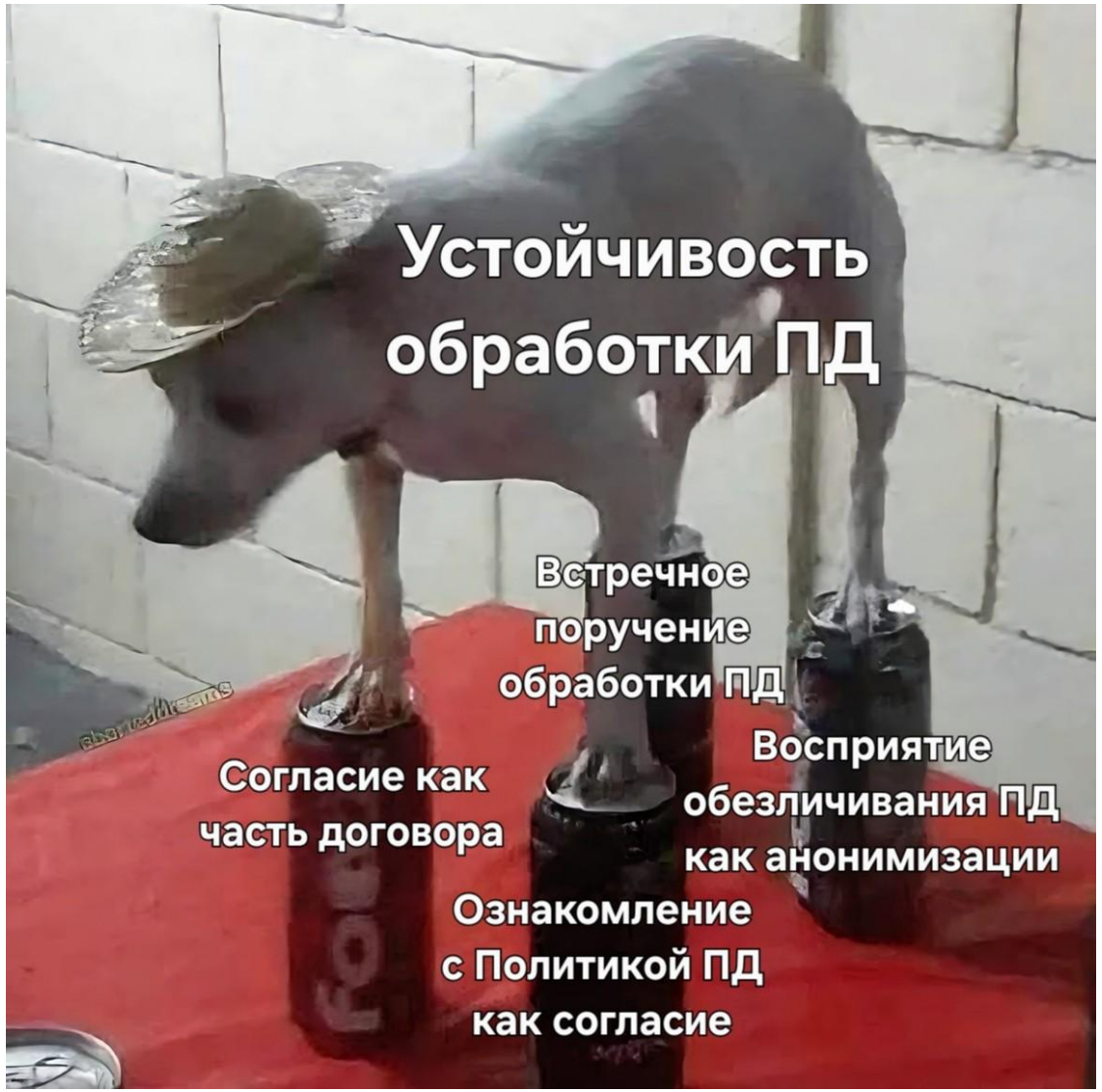
Юмор Альманаха ПД



Privacy Advocates



Privacy Advocates




Однажды все это будет твоим!
Бывалый DPO
Начинающий прайвасист
Корпоративный комплаенс по персональным данным

Privacy Advocates



Privacy Advocates

ПРАЙВАСИСТ ЗАШЁЛ В ОТРАСЛЬ ПРАВА ВНЕ 152-ФЗ



Privacy Advocates

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

ДО УТЕЧКИ	***ПОСЛЕ УТЕЧКИ***
	
Всё ОК	**Всё ОК,** но волнуемся и минимизируем обработку

Privacy Advocates



DPO перед погружением в бизнес-процессы компании

VS.

DPO, разобравшийся в бизнес-процессах компании




2006
2011
2014
2017
2020 – 519-ФЗ
2022 – 266-ФЗ
2023...
Эволюция 152-ФЗ от 27.07.2006 «О персональных данных»

Privacy Advocates



Жизнь DPO

Юмор Альманаха ПД



Privacy Advocates

ОБОЖАЮ РАБОТУ DPO: ЛИБО НИЧЕГО НЕ ПРОИСХОДИТ, ЛИБО ВСЕ ПРОБЛЕМЫ СРАЗУ

Privacy Advocates

Будни DPO и его кота похожи:
шуршишь бумажками,
обедаешь, потом опять
шуршишь бумажками.
Спишь. Иногда шипишь.

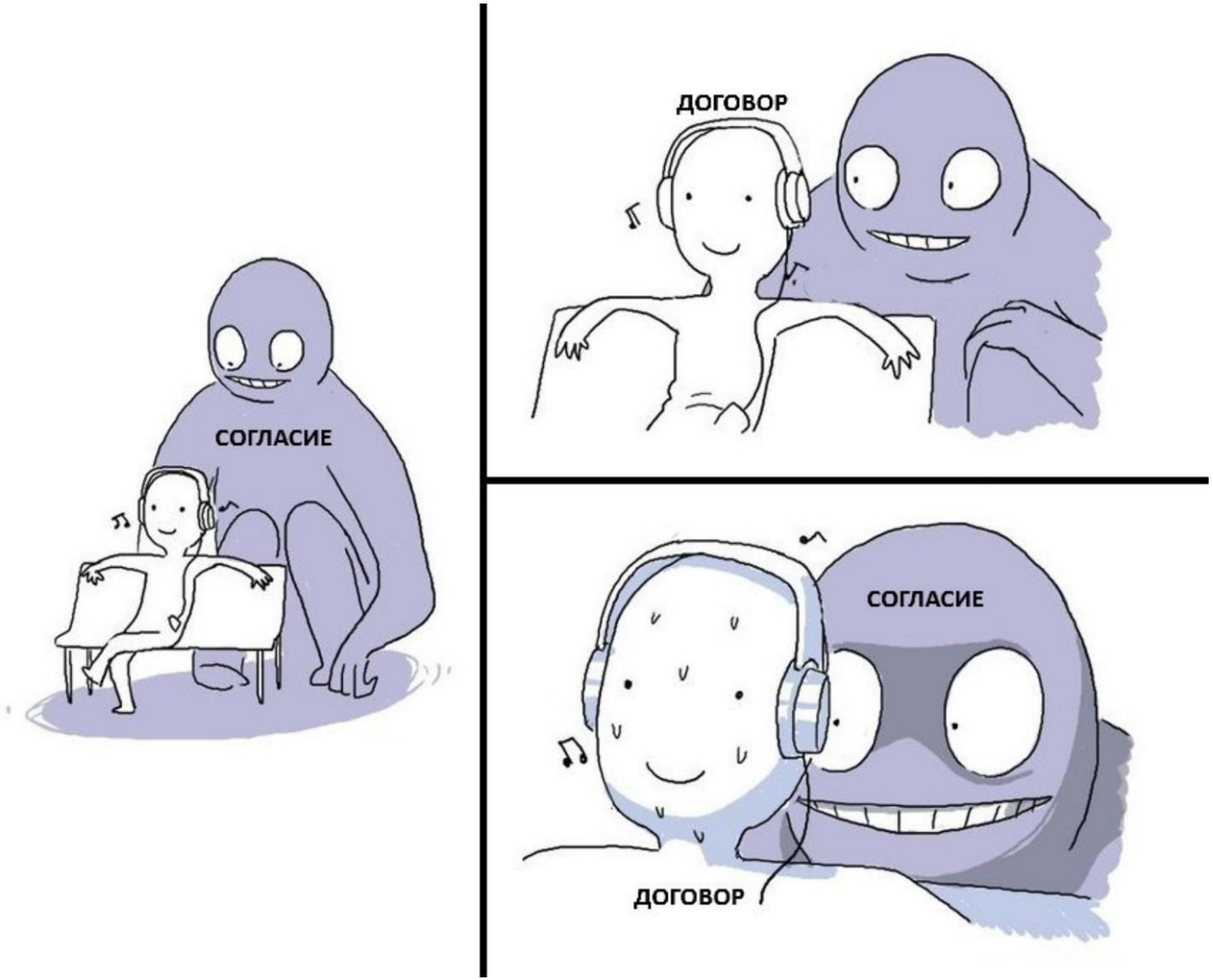
Юмор Альманаха ПД



Privacy Advocates

- Что читаешь?
- 152-ФЗ о персональных данных.
- А чего текст верх ногами?
- Да какая разница!..

Юмор Альманаха ПД



Юмор Альманаха ПД




Nu,Pogodi!
Game A
Game B
Pause
Scores
34
Compliance
Субъекты
Бизнес
Текучка
Будни DPO

Privacy Advocates



Privacy Advocates

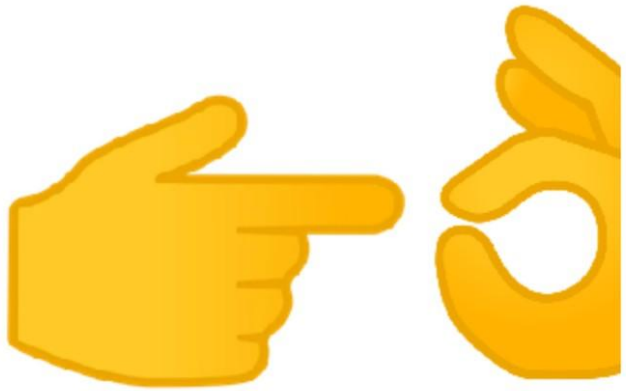
ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫ

ДО УТЕЧКИ



Всё ОК

ПОСЛЕ УТЕЧКИ



Всё ОК,

но чувствуем внимание

Privacy Advocates



Privacy Advocates

Ты не знаешь то, чего не знаешь,
как бы сильно ты не думал.

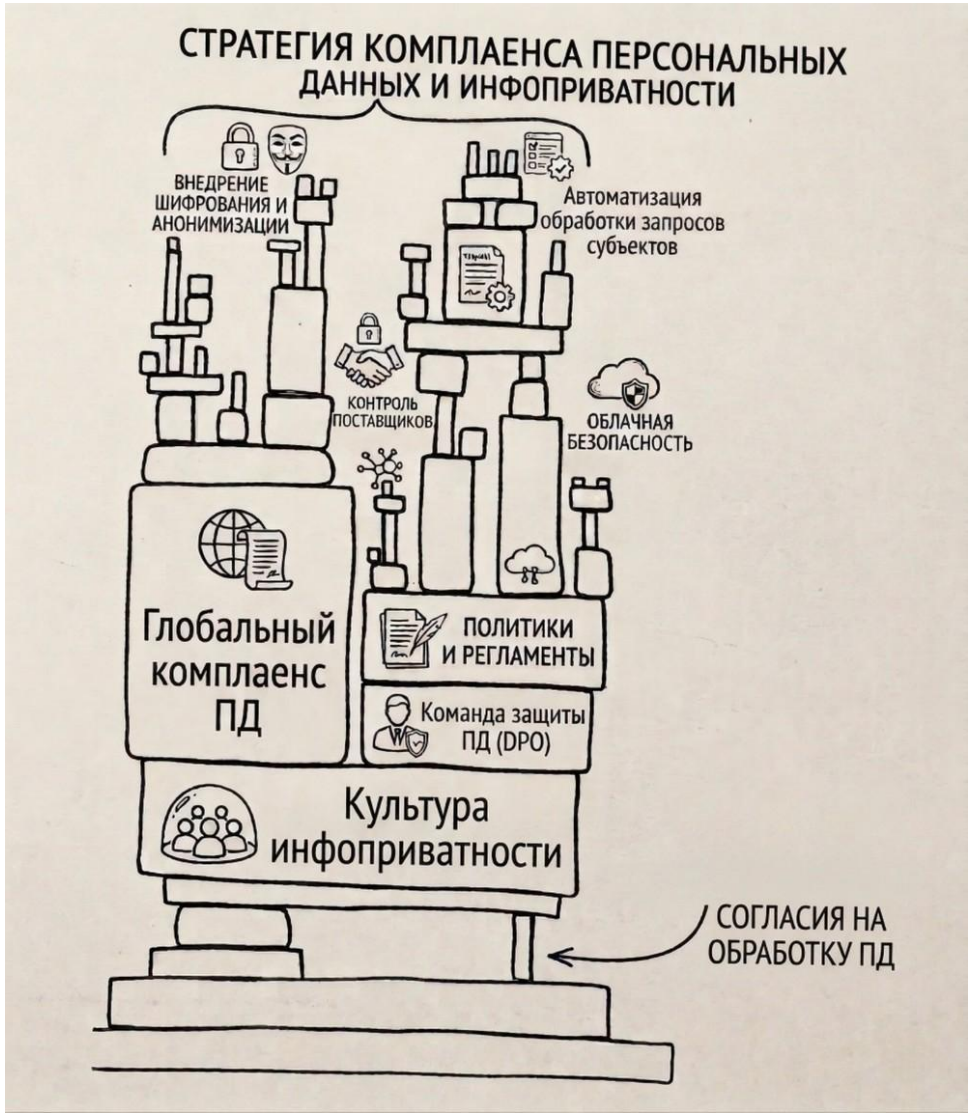


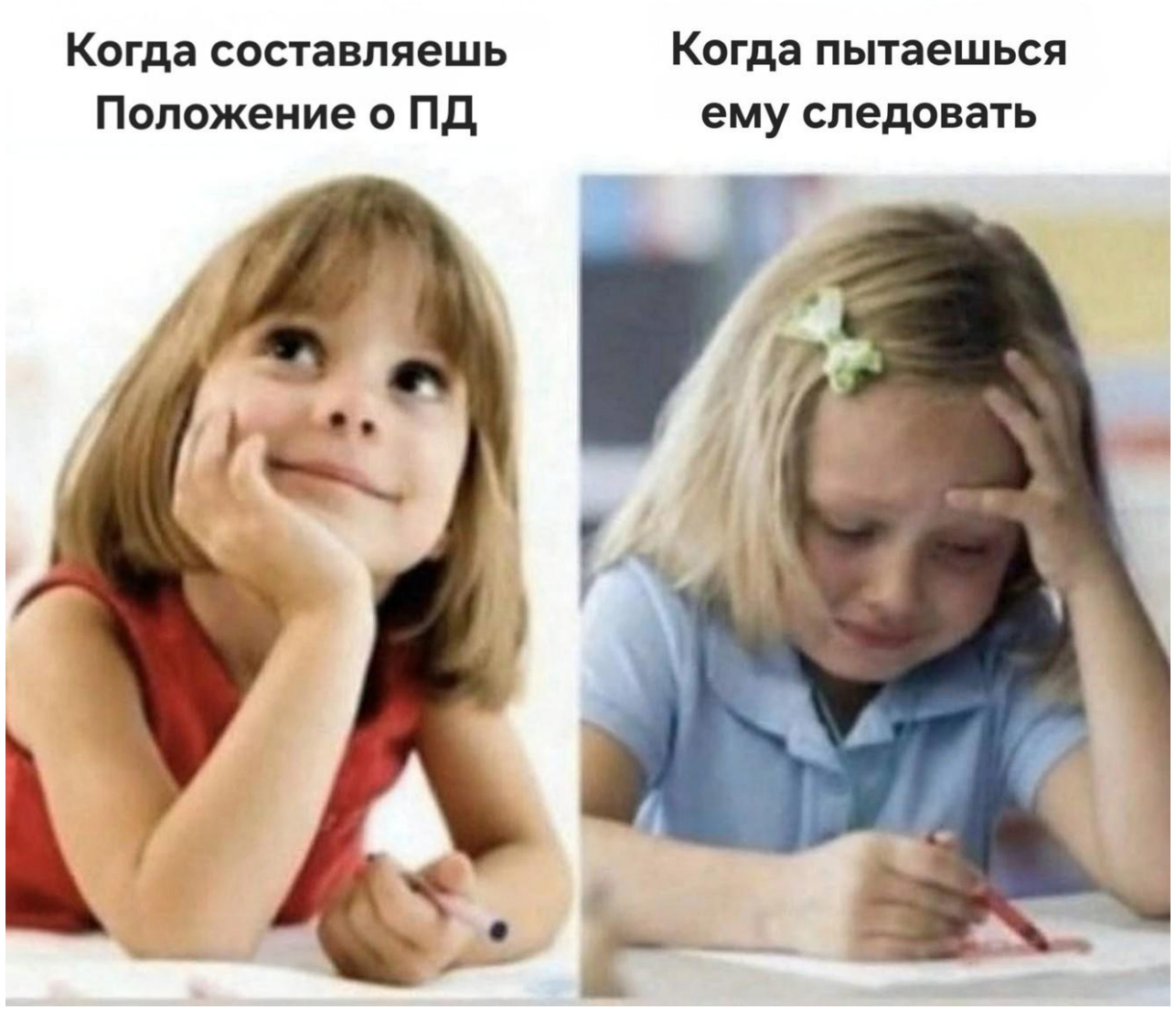
Privacy Advocates



Privacy Advocates




СТРАТЕГИЯ КОМПЛАЕНСА ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНФОПРИВАТНОСТИ
ВНЕДРЕНИЕ ШИФРОВАНИЯ И АНОНИМИЗАЦИИ
Автоматизация обработки запросов субъектов
КОНТРОЛЬ ПОСТАВЩИКОВ
ОБЛАЧНАЯ БЕЗОПАСНОСТЬ
Глобальный комплаенс ПД
ПОЛИТИКИ И РЕГЛАМЕНТЫ
Команда защиты ПД (DPO)
Культура инфоприватности
СОГЛАСИЯ НА ОБРАБОТКУ ПД


Когда составляешь Положение о ПД
Когда пытаешься ему следовать


Я весь такой готовый к
началу работы в роли DPO
Первый день работы DPO

Как описывает вакансию DPO работодатель:



Как это будет на самом деле:




А ты знаешь, что у каждого третьего оператора уже произошла утечка?
У меня нет!
И у меня нет!

Добро пожаловать в комплаенс ПД, у нас сейчас очень интересное время!
Интересное время:



Privacy Advocates

Карта Альманаха

Всегда рады сотрудничеству

corp@privacy-advocates.ru
+7 (903) 762-64-15
t.me/prv_adv