Закон о персональных данных: что знать и как быть

Comply.

О спикере

Сергей Сайганов

Comply. | Партнер и сооснователь
SmartКЭДО | CEO

e-mail: sergei@comply.ru
tg: t.me/saiganov

- более 10 лет юридической практики
- DPO в ряде компаний, вкл. Melon Fashion Group
- ex-Group-IB и PricewaterhouseCoopers
- Tier-1 Право.Ру-300, Коммерсант, RPPA
- специализируюсь на технологических компаниях и проектах
- CEO системы КЭДО **Smart**КЭДО и смежных продуктов

ПРАВО.RU 300 РЕЙТИНГ ЮРИДИЧЕСКИХ КОМПАНИЙ РОССИИ

Коммерсантъ

Russian Privacy Awards

РБК

ПРЕМИЯ РУНЕТА

План

1	Введение	10′
2	Ключевые риски	20′
3	Управление рисками	30′
4	Законность обработки	30′
5	Внутренние контроли и процедуры	20′
6	Privacy & AI	10′

1

Введение

- Чем регулируется
- Что такое ПД
- Кто субъекты ПД

Что такое ПД? [1]

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

≠ точно идентифицирующая конкретного человека

= которую можно ассоциировать с человеком

- **Критическая** масса
- **Контекст** обработки

} **Риск-аппетит компании**

Адрес места жительства
Возраст
Дата рождения
Время просмотра web-страницы
Серия и номер паспорта
ИНН
ФИО
IP-адрес
HTTP Cookie
Номер телефона
Фото- и видеоизображение
Аккаунты соцсетей
Логин учетной записи
Друзья / родственники
СНИЛС
Должность и место работы
e-mail
Геоидентификатор
GA ID / IDFA
HTTP referer
Вектора, скоринги, эмбединги
Хэш-ID пользователя
ID в системах
Геолокация

comply.ru | t.me/comply_ru | info@comply.ru

Comply.

Что такое ПД? [1]

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

~~Общедоступные~~ разрешенные данные:

- из соцсетей
- из публичных реестров
- из визиток и иных источников

- E-mail признан и не признан судом ПД
- Cookie-файлы признаны судом ПД и тут
- Номер телефона считается и не считается ПД

- Хеширование данных – средство защиты ПД, а не обезличивания
- Проект приказа РКН с требованиями и методами обезличивания
- Обезличенные ПД – все равно ПД
- Непонятен момент перехода, когда ПД теряют статус ПД – проблема актуальна даже для синтетических данных
- Синтетические данные, вектора / эмбединги, соль переменная, BlackBox / анклавы – серая зона

Особые виды ПД

99% Необходимо строгое письменное согласие

Специальные | Биометрические | Разрешенные для распространения | ПД несовершеннолетних

- Состояние здоровья
- Интимная жизнь
- Расовая, национальная принадлежность
- Политические взгляды
- Религиозные или философские убеждения
- Сведения о судимости

...

- Сведения о нетрудоспособности – спец. категория
- Сведения об инвалидности – спец. категория; социальный статус, а не спец. категория
- Сведения о судимости – в зависимости от детализации

РКН требует обоснования необходимости обработки спец. категорий ПД, а также закрепления порядка такой обработки в ЛНА

Особые виды ПД

99% Необходимо строгое письменное согласие

Специальные | **Биометрические** | Разрешенные для распространения | ПД несовершеннолетних

› **Характеризуют** физиологические и биологические особенности человека

› На основании ПД **можно установить** личность субъекта и **используется** для этого

› Примеры:

- Изображение лица
- Запись голоса
- FaceID
- TouchID
- Сетчатка глаз
- Рисунок вен
- Видеозапись с камер видеонаблюдения
- Фотография в загран. паспорте

...

- Фото на пропуске признано судом биометрией
- Фото в СКУД признано и не признано РКН биометрией

Если в документах компании данные определены как биометрические, то Роскомнадзор может потребовать соблюдения условий обработки биометрических ПД

Особые виды ПД

Специальные | **Биометрические** | Разрешенные для распространения | ПД несовершеннолетних

Примеры:

- Изображение лица
- Запись голоса

Единая биометрическая система

- FaceID ✓
- TouchID ✓
- Сетчатка глаз ✓
- Рисунок вен ✓
- Видеозапись с камер видеонаблюдения ✓

Обработка биометрических ПД (изображение лица, запись голоса) вне ЕБС / КБС почти всегда запрещена.

Возможные варианты:

- отказаться от обработки биометрии и отслеживать законодательные изменения
- обратиться к провайдеру, который может правомерно организовать обработку
- не квалифицировать Face ID как биометрию во внутренних документах Компании, а только в качестве «математических преобразований»
- исключить идентификацию / аутентификацию

Особые виды ПД

Оператор может получить рекомендацию РКН по своей форме согласия

Специальные | Биометрические | Разрешенные для распространения | ПД несовершеннолетних

Условия обработки:

Субъект предоставил согласие на распространение его ПД в публичных источниках

Обработка ПД, получаемых из публичных источников, не нарушает условия, поставленные субъектом, и не выходит за рамки целей согласия

В источнике опубликованы условия и запреты дальнейшей обработки

...

- Можно публиковать без согласия, если этого требует закон (например, ПД врачей на сайте больницы по ч. 7 ст. 21 323-ФЗ) или если это предусмотрено иным основанием п. 2-11 ч. 1 ст. 6 152-ФЗ

Согласие на распространение – ~~единственное~~ основание обработки.

Получается отдельно, должно соответствовать форме РКН и позволять субъекту определять условия и запреты дальнейшего распространения

Особые виды ПД

Условия обработки:

Родитель или иной законный представитель предоставил **согласие** на обработку ПД

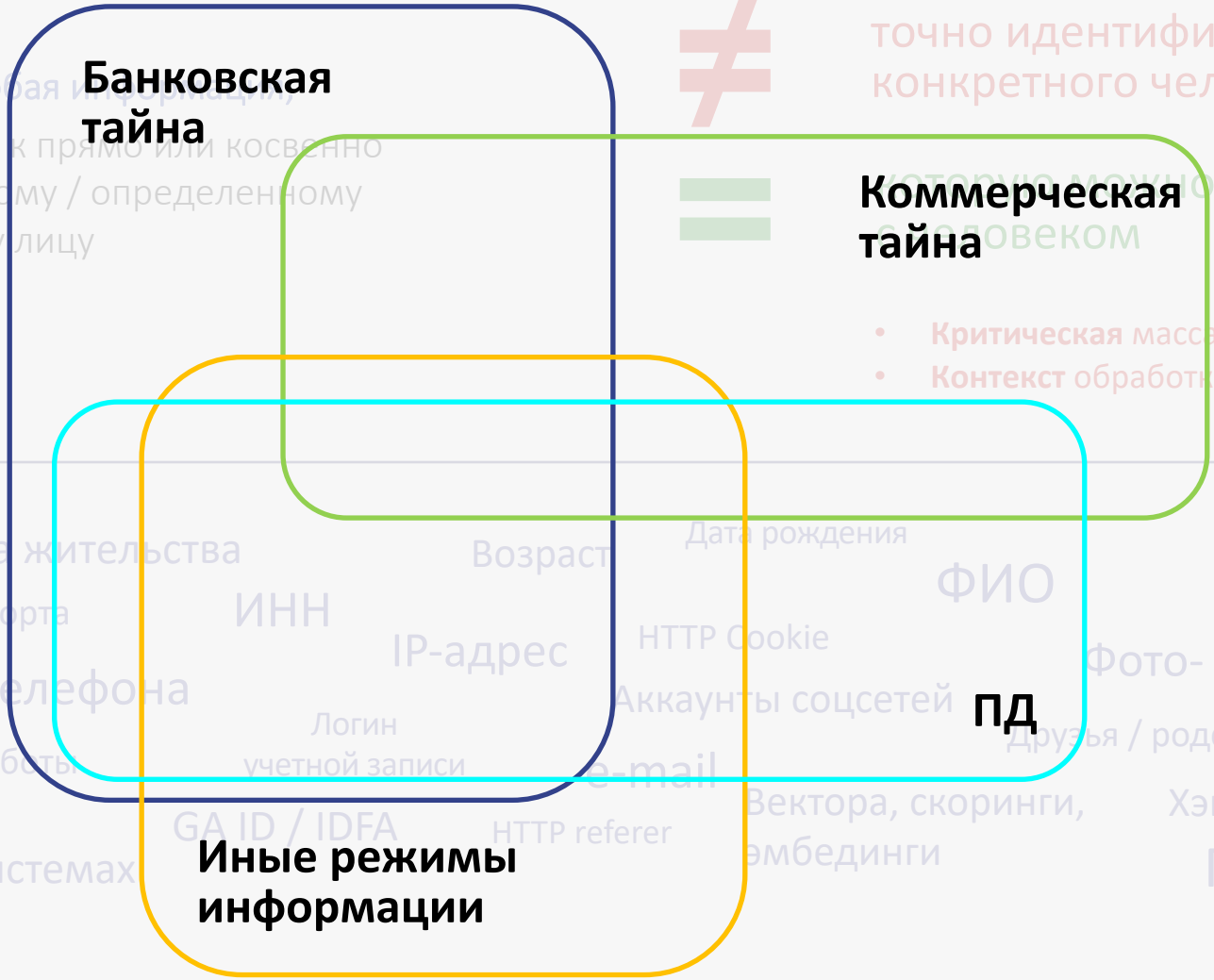
Обработка осуществляется на основании договора с несовершеннолетним либо ином законном основании

Несовершеннолетними для целей обработки ПД признаются лица, не достигшие возраста **14 лет**

Позиция Роскомнадзора 18.02.2022: при определении объема дееспособности ориентируемся на положения ГК РФ:

- до 14 лет – согласие дают родители
- после 14 лет – сам несовершеннолетний

Что такое ПД? [2]



≠

точно идентифицирующая конкретного человека

=

которую можно ассоциировать с человеком

- **Критическая** масса
- **Контекст** обработки

Риск-аппетит компании

comply.ru | t.me/comply_ru | info@comply.ru

Comply.

Кто может быть субъектом ПД?

- Кандидаты на вакантные должности
- Работники
- Бывшие работники
- Родственники работников
- Стажеры и практиканты
- Клиенты и их представители
- Участники мероприятий
- Посетители офисов
- Посетители сайтов
- Партнеры и иные контрагенты
- Представители контрагентов
- ГПХ-подрядчики
- Бенефициары
- Работники компаний группы

Что такое обработка ПД?

Обработка ПД – любое действие с ПД с использованием средств и без использования автоматизации.

Источники ПД и ресурсы, где они хранятся

Информационные системы

- Базы данных
- Серверы
- Рабочие станции
- Сетевая инфраструктура

Бумажные носители

- Журналы
- Анкеты
- Визитные карточки
- Договоры

Электронные носители

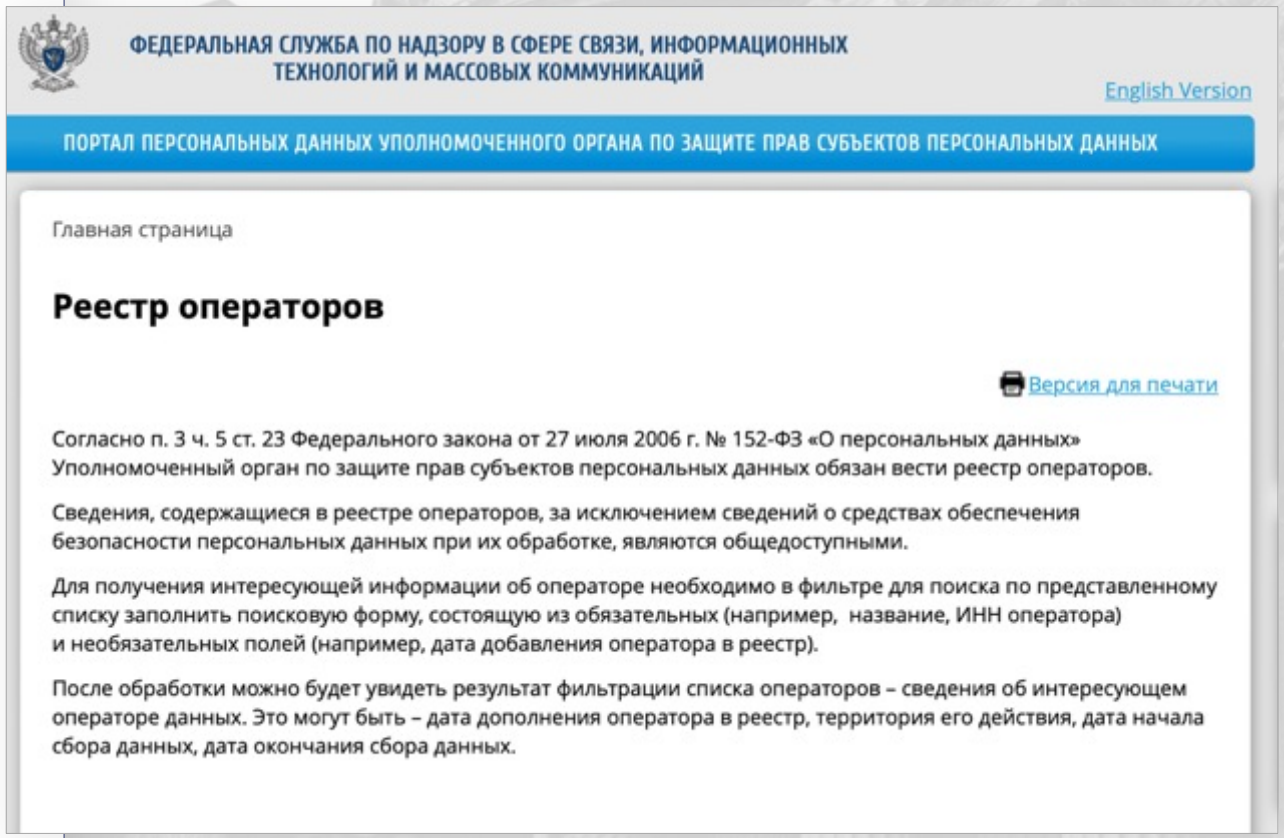
- Магнитные ленты
- Флеш-носители
- Оптические диски

Кто такой Роскомнадзор, и что у него за реестр?

Федеральная служба по надзору в сфере связи, ИТ и массовых коммуникаций

Роскомнадзор (РКН) является владельцем реестра операторов персональных данных (ПД), в том числе отвечает за:

- наполнение реестра и регистрацию операторов
- контроль поданных сведений
- периодическое обновление сведений



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

Реестр операторов

Версия для печати

Согласно п. 3 ч. 5 ст. 23 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» Уполномоченный орган по защите прав субъектов персональных данных обязан вести реестр операторов.

Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

Для получения интересующей информации об операторе необходимо в фильтре для поиска по представленному списку заполнить поисковую форму, состоящую из обязательных (например, название, ИНН оператора) и необязательных полей (например, дата добавления оператора в реестр).

После обработки можно будет увидеть результат фильтрации списка операторов – сведения об интересующем операторе данных. Это могут быть – дата дополнения оператора в реестр, территория его действия, дата начала сбора данных, дата окончания сбора данных.

Кто такой оператор ПД?

ВСЕ КОМПАНИИ | независимо от организационно-правовой формы | ООО, АО и даже ИП

Любая компания является **оператором ПД**, т.к. обрабатывает ПД:

- сотрудников
- учредителей
- клиентов
- представителей контрагентов

В законе нет понятия «регистрация в качестве оператора ПД» – компания / ИП является оператором автоматически с момента начала обработки ПД

Независимо от факта регистрации в реестре РКН

Чем регулируется?

Нормы права

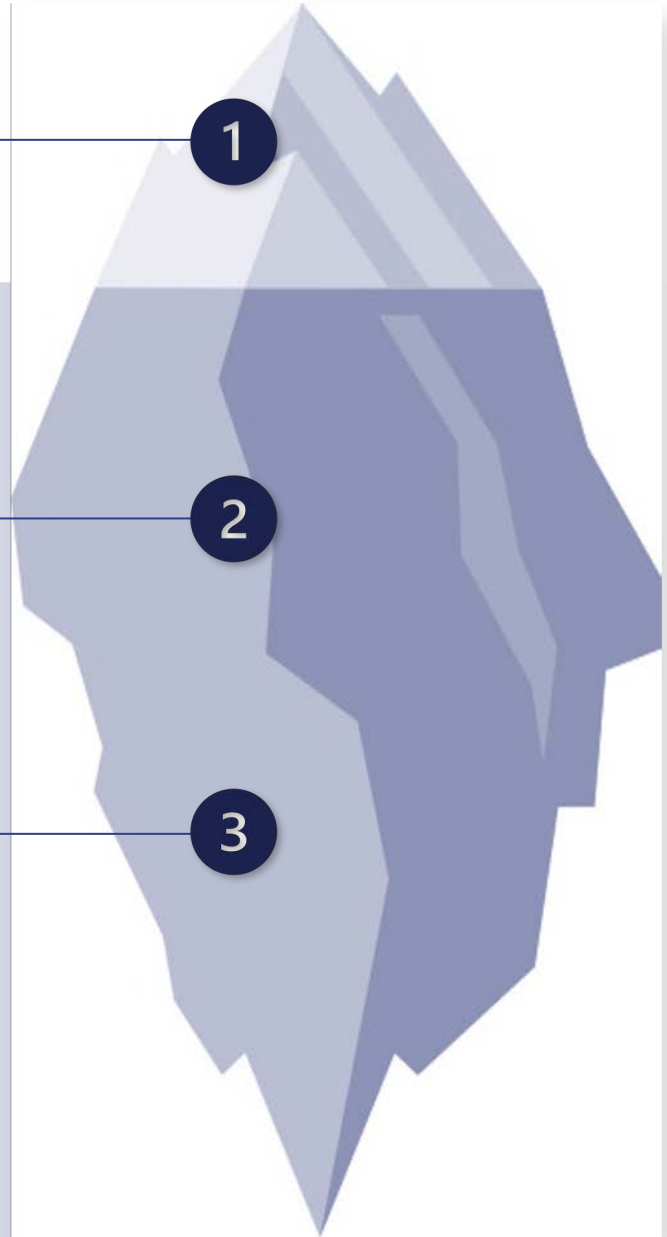
152-ФЗ, 149-ФЗ, 38-ФЗ
ПП РФ №№ 1119, 687
Указ № 250, Приказы РКН, ФСТЭК
395-1-ФЗ, 115-ФЗ, Положение ЦБ РФ № 499-П, Стандарты ЦБ РФ

Практика

Официальные разъяснения Роскомнадзора, письма ЦБ, ФАС и судебная практика

«Динамичное» право

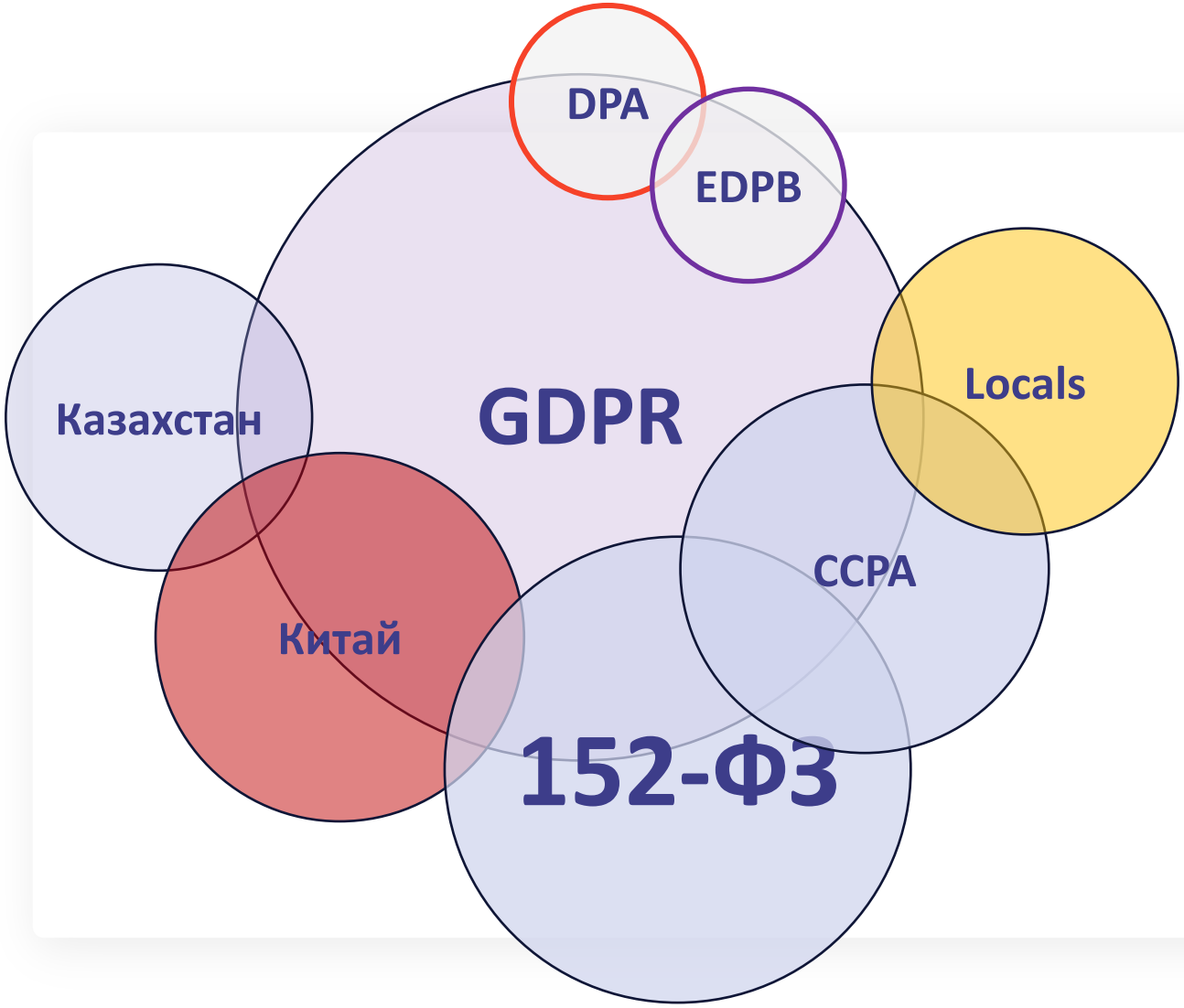
Устные комментарии РКН, позиции в предписаниях РКН, ФАС



Примеры

- Портал Роскомнадзора по ПД, вкладка "Новости"
- Telegram-канал Роскомнадзора
- Сообщество Роскомнадзора в VK
- Видеозапись дня открытых дверей РКН 27.07.2023
- Видеозапись дня открытых дверей РКН 01.03.2023
- Инсайдер РКН
- Анализ правоприменительной практики
- Письмо Роскомнадзора от 07.02.2014 № 08КМ-3681 "О передаче работодателем третьим лицам сведений о заработной плате работников"
- Ответы на вопросы в сфере защиты прав субъектов ПД
- Памятки операторам обработки ПД по разным вопросам обработки ПД
- Информационное письмо Банка России N ИН-06-59/57 и РКН N 08ЛА-48666 от 29.07.2021 "О согласии заемщиков на обработку их персональных данных"
- Информационное письмо Банка России N ИН-06-59/70 и ФАС России N АК/75514/21 от 06.09.2021 "О согласии на получение рекламы"
- Стандарт Банка России СТО БР БФБО-1.8-2024

Privacy-регулирование



Важна оценка применимости, т.к. может применяться экстерриториально:

- прямая (направленность)
- договорная

Различия в подходах, риски

Privacy – зона турбулентности

2

Ключевые риски

- Бизнес
- Работники
- Новые риски

Ключевые риски для компании [1]

ФИНАНСОВЫЕ

- Штрафы до 500 тыс. руб.
- Кратное применение
- Штраф за нелокализацию ПД до

Иные нарушения

- Нет надлежащего основания обработки ПД – 300 / 500 тыс. руб.
- Нет письменного согласия на обработку ПД – 700 / 1.500 тыс. руб.
- Нет политики об обработке ПД – 60 тыс. руб.
- Нарушение процедуры ответа на запросы – 80 тыс. руб.
- Непрекращение обработки ПД – 90 / 500 тыс. руб.
- Нелокализация ПД до 18 млн. руб.
- Размещение биометрии в ЕБС с нарушениями – 1 млн. руб.
- Нарушение требований о защите информации – 100 тыс. руб.

Утечки ПД

1-я утечка — до **15 млн** руб.

Субъектов ПД	Штраф
1 000 - 10 000	3 - 5 млн руб.
10 000 - 100 000	5 - 10 млн руб.
более 100 000	до 15 млн руб.

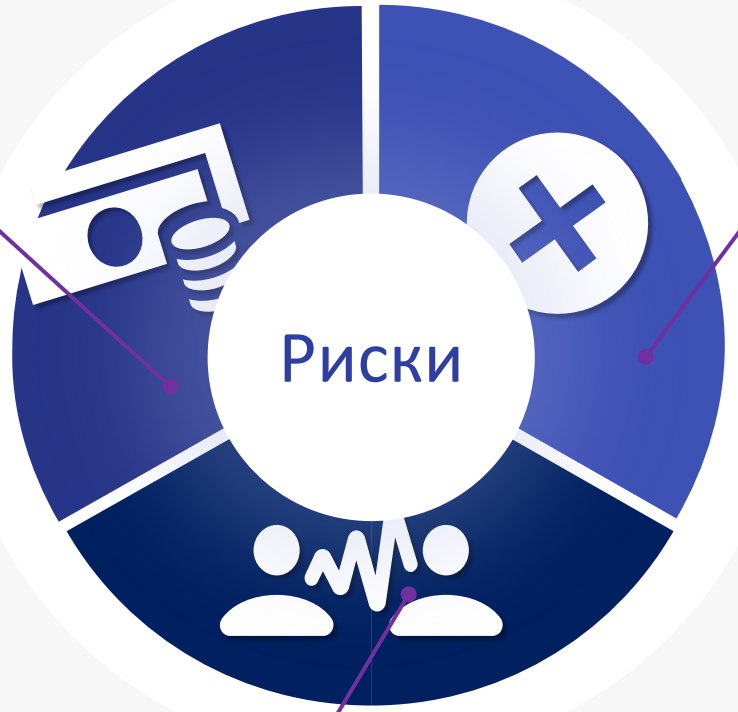
2-я утечка — до **500 млн** руб.

0,1 – 3 % от выручки за год / 15 – 500 млн руб.

Неуведомление РКН — до **3 млн** руб.

Штраф до 300 тыс. руб.
за невключение в реестр операторов РКН

Ключевые риски для компании [2]



ФИНАНСОВЫЕ

- Штрафы
- Кратное применение
- Коллективные иски
- Компенсация субъектам

Субъект совместно с ГРЧЦ взыскали с банка 100 тыс. руб. моральной компенсации за неправомерную передачу ПД

ОРГАНИЗАЦИОННЫЕ

РЕПУТАЦИОННЫЕ

- Лояльность клиентов / работников
- Доверие инвесторов
- GR / риск-группы

Ключевые риски для компании [3]

1. **в пятидневный срок** со дня получения настоящего Предписания прекратить нарушение законодательства Российской Федерации о рекламе, а именно прекратить распространение ненадлежащей рекламы посредством использования телефонной связи, в том числе на телефонный номер с нарушением частей 1,2 статьи 18 Закона о рекламе, а также прекратить распространение рекламы в нарушение части 1 статьи 18 Закона о рекламе иным лицам, не предоставившим выраженного согласия именно на получение рекламы от конкретного рекламораспространителя

в течение 6 месяцев изменить правила работы с персональными данными субъектов персональных данных в информационных системах оператора персональных данных. Обеспечить уничтожение персональных данных из информационных систем в сроки, предусмотренные требованиями законодательства, в случае достижения цели обработки персональных данных и при отсутствии иных оснований обработки персональных данных.

ОРГАНИЗАЦИОННЫЕ

- Запрет обработки ПД
- Необходимость сбора новых согласий
- Блокировка сайта и проблемы с app-сторами
- Изменения ИТ-ландшафта
- Ликвидация компании за неоднократное нарушение

Comply.

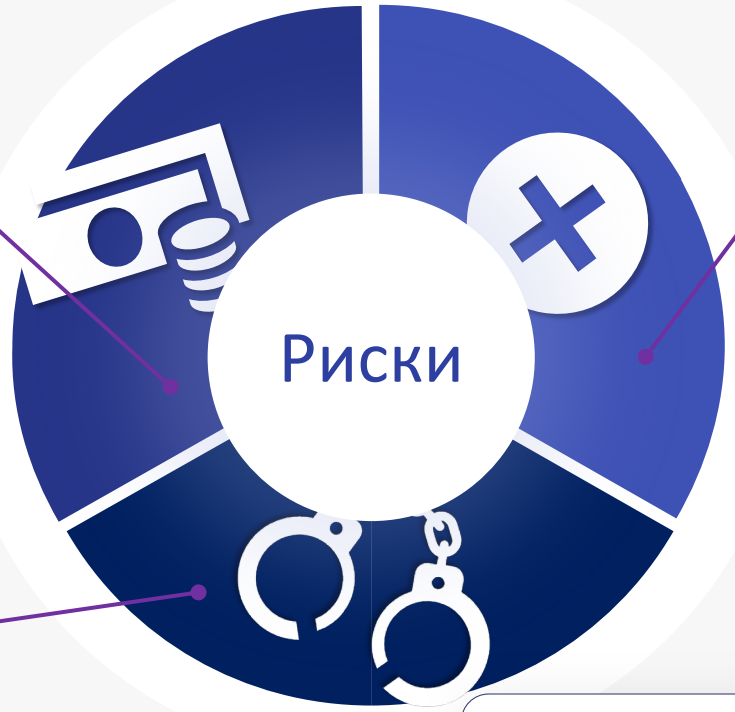
Ключевые риски для работников [1]

ФИНАНСОВЫЕ

- Штрафы до 500 тыс. руб. (до 50 тыс. руб. за ИБ нарушения)
- Штраф за нелокализацию ПД до 800 тыс. руб
- Кратное применение

УГОЛОВНЫЕ

- Незаконная обработка ПД: до 4 лет
- Нарушение неприкосновенности частной жизни: лишение свободы до 2 лет
- Неправомерный доступ к компьютерной информации: лишение свободы до 7 лет



ОРГАНИЗАЦИОННЫЕ

- Дисквалификация на срок до 3 лет
- Проблемы с продлением и получением визы

Штраф DPO за утечку ПД:

- Постановление Мирового судьи судебного участка № 360 г. Москвы от 6 декабря 2023 г. по делу № 05-0956/360/2023
- Решение Московского городского суда от 11 октября 2023 г. по делу № 7-21402/2023

Comply.

Ключевые риски для работников [2]

Новый состав уголовной ответственности – ст. 272[1] УК РФ

Состав	Ответственность
Незаконные **использование** и (или) передача, сбор или **хранение** ПД, **полученных** путем неправомерного доступа или **иным незаконным путем**	• штраф до 300k или годовой доход, либо • принудительные работы до 4 лет, либо • лишение свободы до 4 лет
То же самое, но в отношении ПД **несовершеннолетних, специальных категорий** ПД или биометрии	• штраф до 700k или в размере дохода за 2 года с/без лишением права занимать определенные должности или деятельностью либо • принудительные работы до 5 лет, либо • лишение свободы до 5 лет
Создание ресурсов, предназначенных для распространения ПД	• штраф до 700к либо • лишение свободы до 5 лет с запретом занимать должность до 2 лет
Дополнительные признаки: трансграничная передача, организованная группа лиц, тяжкие последствия	• штраф до 3 млн, либо • лишение свободы до 10 лет

К ответственности может быть привлечен при наличии умысла (от более вероятного к менее вероятному):

- ГД
- исполнитель утечки (например, внутренний инсайдер)
- рук-ль подразделения, инициирующий обработку
- DPO

Ключевые риски для работников [3]

Новый состав уголовной ответственности – ст. 272[1] УК РФ

ТАСС

28 февраля 2025 / 19 марта 2025

У TG-бота «Глаз бога» прошли обыски по первому делу о незаконном использовании ПД

Первый случай применения ст. 272.1 УК в отношении работника салона сотовой связи за «слив» ПД

15 января 2025

Условием ответственности по ст. 272.1 УК РФ … двух составляющих:

- незаконный способ завладения
- незаконные действия по распространению

11 марта 2025

Криминализация:

- неправомерного доступа, в результате которого ПД неправомерно обрабатываются
- сервисов пробива

🔥 **Широкое толкование** объективной стороны

п. 5 постановления Пленума ВС РФ № 37

🔥 Риски для **менеджмента** при соучастии

ст. 32 УК РФ

Ключевые риски для работников [3]

Новый состав уголовной ответственности – ст. 272^1 УК РФ

14 ноября 2025

- Главу пресс-службы петербургского ГУ МВД отправили под домашний арест по обвинению ч.6 ст.272.1 и ч.5 ст.290 УК РФ

- С 2022 года администратор новостного канала "Конкретно.ру" на систематической основе передавал взятки за предоставление ежедневных сводок происшествий ведомства и видео событий, зафиксированных камерами наблюдения городского мониторингового центра.

- Оба среди прочего обвиняются в создании и обеспечении функционирования информационного ресурса, заведомо предназначенного для незаконного хранения и передачи компьютерной информации, содержащей персональные данные и полученной незаконным путем (ч. 6 ст. 272.1 УК РФ).

Ключевые риски для работников [3]

Новый состав уголовной ответственности – ст. 272^1 УК РФ

1 ноября 2025

- В Москве задержан владелец бота по поиску персональных данных Userbox
- Предъявлено обвинение по ст. 272.1 УК РФ «Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные».
- Ранее по аналогичным статьям задержали владельцев ботов для пробива Solaris Inform и TeleSINT.
- Userbox (также известен как User_Search) считается альтернативой телеграм-бота «Глаз Бога», который перестал работать в феврале 2025 года.

Ключевые риски для работников [4]

Сценарии обработки ПД	Риск	Незаконное получение	Мало-значительность	Исходная законность	Вероятность наступления
Исходно без правового основания	ВЫСОКИЙ	+	-	-	+
С согласием, однако полученным с нарушением установленного порядка	СРЕДНИЙ	+	+/-	+/-	+
По истечении срока действия основания	СРЕДНИЙ	+/-	+	+	+/-
После отзыва согласия на обработку ПД	СРЕДНИЙ	+/-	+/-	+/-	+
Техническая ошибка (ошибочное логирование факта предоставления согласия)	НИЗКИЙ	-	+	+	+/-
Внешнее воздействие (хакерская атака)	НИЗКИЙ	-	+	+	+

Ключевые риски для работников [5]

Должность / роль работника	Риск	Конкретные действия	Доступ к ПД	Корыстная мотивация	Осознание
ЕИО / председатель, члены коллегиального органа	НИЗКИЙ	-	-	+	+/-
Руководители структурных подразделений	НИЗКИЙ	-	-	+/-	+/-
Руководители отдельных проектов/процессов	СРЕДНИЙ	+/-	+/-	-	+
Исполнители в рамках отдельных проектов/процессов	ВЫСОКИЙ	+	+	+	+
Специально указанные во внутренних документах компании ответственные лица проектов/процессов, включая DPO	ВЫСОКИЙ	+/-	+	-	+
Члены риск-комитетов, риск-чемпионы	СРЕДНИЙ	+/-	-	+	+

3

Управление рисками

- Оборотные штрафы за утечки
- Уголовная ответственность

Риск-ориентированный подход

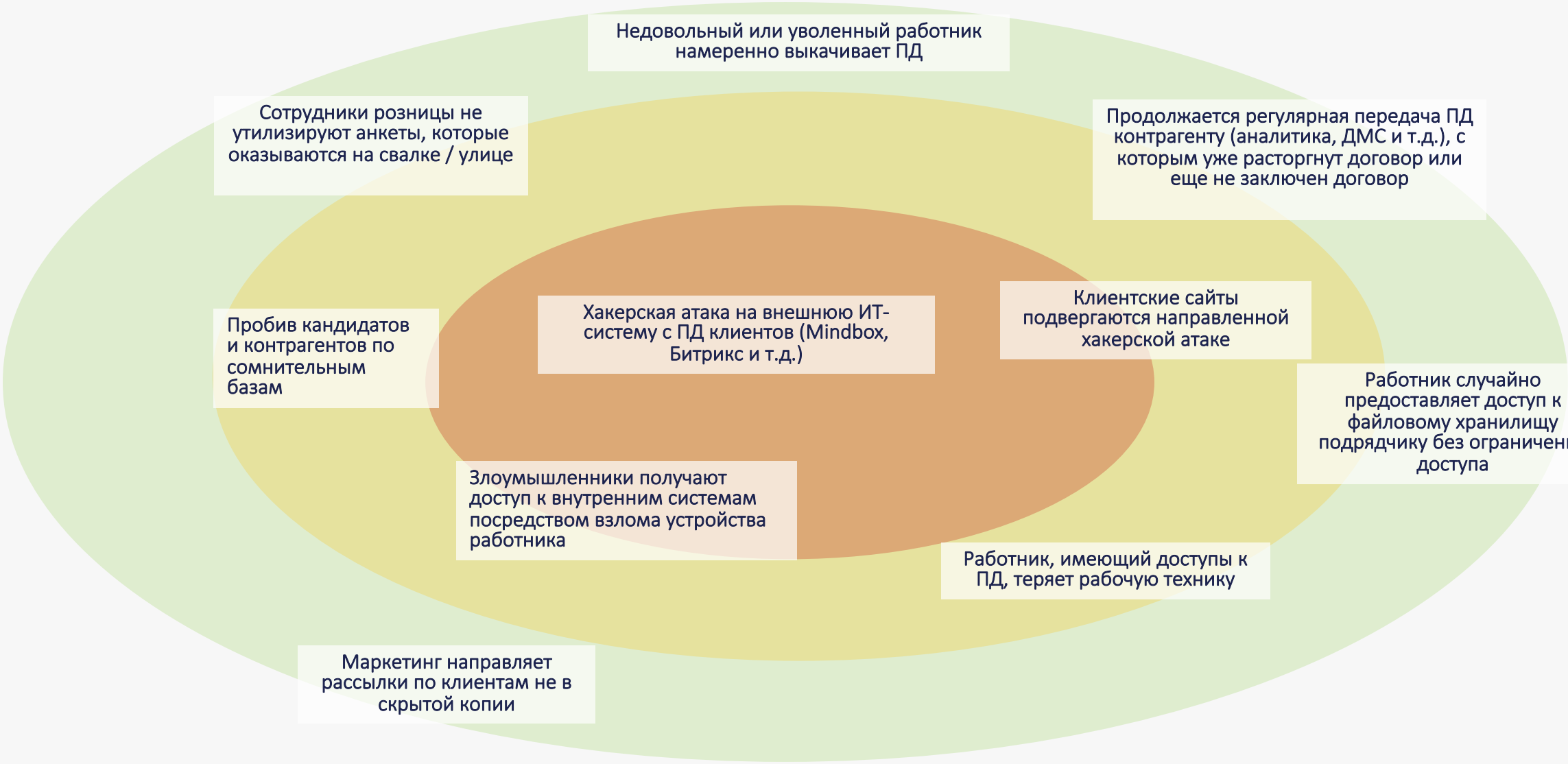
BACK OFFICE

- Инциденты с ПД из-за внутреннего или внешнего нарушителя:
  - Оборотные штрафы
  - Уголовные риски
- В 2023 – 2024 г. в России утекло более 1,5 млрд записей (592 инцидента)
- Если РКН после 30 мая узнает про утечку, произошедшую до 30 мая, то компанию тем не менее оштрафуют по новым штрафам

FRONT OFFICE

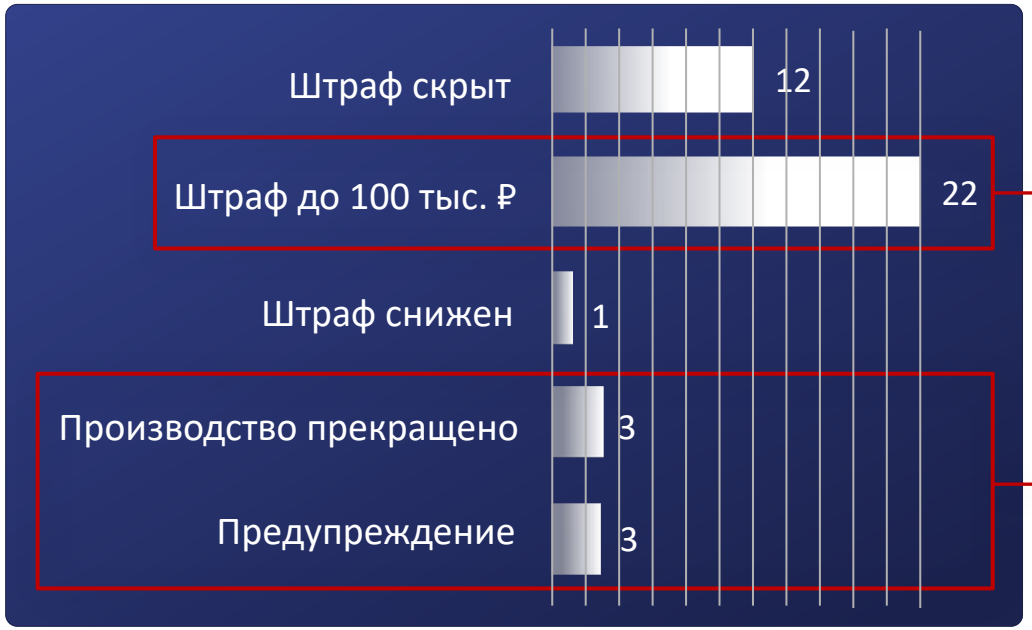
- Очередное расширение перечня индикаторов риска – основание для проведения внеплановой проверки РКН
- Конец моратория на внеплановые проверки (п. 3 ПП № 336)
- Интенсификация дистанционного контроля РКН – 3+ тыс. мероприятий / год и до 0,5 млн плановая пропускная способность
- **+30%** ежегодно прирост кол-ва **жалоб** в ФАС и РКН

Зоны риска и сценарии



Comply.

Оборотные штрафы [1]



В том числе 1) **МТС-Банк** (Постановление Мирового судьи судебного участка № 248 г. Москвы от 27 ноября 2023 г. № 5-1189/23), 2) **АКБ реконструкции и развития** (Постановление Мирового судьи судебного участка № 4 Волжского района г. Саратова от 17 апреля 2024 г. № 5-301/24)

Производство прекращено - 1) ООО "**Спортмастер**" (Постановление Мирового судьи судебного участка № 52 г. Москвы от 5 июня 2023 г. № 5-309/23), 2) СПАО "**Ингосстрах**" (Решение Замоскворецкого районного суда г. Москвы от 15 июня 2023 г. по делу № 12-1105/2023), 3) АО "**АльфаСтрахование**" (Постановление Мирового судьи судебного участка № 244 Донского района г. Москвы от 25 сентября 2023 г. № 5-1048/23)

Предупреждение - 1) ООО "**СКИ ПЛЮС**" (Постановление Мирового судьи судебного участка № 4 Ленинского района г. Пензы Пензенской области от 5 августа 2024 г. № 5-338/24), 2) АО СК "**БАСК**" (Постановление Мирового судьи судебного участка № 7 Беловского городского судебного района Кемеровской области от 13 июня 2024 г. № 5-494/24), 3) ООО "**ТД "Аскона**" (Постановление Мирового судьи судебного участка № 9 г. Коврова и Ковровского района Владимирской области от 30 августа 2023 г. № 5-234/23)

НОВЫЙ КОНТЕКСТ

- Рассмотрение дел арбитражными судами
- Специальные смягчающие обстоятельства для повторных утечек: (а) инвестиции в ИБ в размере, (б) оценка эффективности СЗИ

Оборотные штрафы [2]

НЕПРАВИЛЬНО

- Неуведомление РКН – риск получить проверку РКН и штраф
- Хакер – НЕ оправдание
- Внедрение отсутствующих СЗИ – НЕ оправдание

РЕАГИРОВАНИЕ

- Ограничение доступов / смена паролей
- Мониторинг публикаций дампов
- Заявление о преступлении
- Усиление контроля за DSR и реестр
- Расторжение договора с вендором
- PR и компенсации субъектам

СТРАТЕГИЯ

- План, RACI
- Учения
- Новый подход к договорам для распределения рисков с партнерами
- Кибер-страховка

Бургер Кинг x **РКН** по утечке Майндбокс

Постановление Мирового судьи участка № 416 г. Москвы от 21 января 2025 № 5-902/24

Оборотные штрафы [3]

Чек-лист

Контроль	Артефакт	Скоринг	Домен
• **Регулярный контроль процессов обработки ПД**	• План и акты внутренних проверок ПД • Планы устранения выявленных нарушений • Отчеты об устранении выявленных нарушений	ВЫСОКИЙ СРЕДНИЙ НИЗКИЙ	DPO
• Актуализация ЛНА, RoPA, сведений в реестре			
• Контроль внедрения новых процессов, ИТ-систем			
• **Privacy-контроль контрагентов**	• Стандартные оговорки о ПД в договоры с контрагентами • Регламент privacy-проверки новых контрагентов • Заполненные анкеты новых контрагентов и их обновление • Иные артефакты проверки контрагентов (переписка и т.п.) • Privacy-playbook по привлечению контрагентов	ВЫСОКИЙ СРЕДНИЙ НИЗКИЙ НИЗКИЙ НИЗКИЙ	DPO+ИБ
• Внедрение и периодический контроль системы защиты ПД			
• Минимизация обрабатываемых ПД			
• Контроль доступа к данным			
• **Проверка знаний работников**	• Процедура информирования РКН и иных регуляторов об инциденте • Акты о проведении учений по реагированию на инциденты • Privacy-playbook по процедурам реагирования в случае утечки ПД	ВЫСОКИЙ СРЕДНИЙ НИЗКИЙ	DPO+ИБ
• Внедрение и тестирование рабочих процедур и контролей по реагированию на инциденты			

Оборотные штрафы [4]

ПОЗИЦИЯ ДЛЯ РКН И СУДА

СОДЕРЖАНИЕ ИНЦИДЕНТА	ОБЪЕКТИВНАЯ СТОРОНА ИНЦИДЕНТА	РЕАГИРОВАНИЕ НА ИНЦИДЕНТ
относительно небольшой **масштаб** инцидента	**первый** инцидент, оператор **добросовестно** выполнял требования	своевременно и должным образом **уведомлены**
нет специальных и биометрических **категорий**	инцидент вследствие **эксцесса исполнителя** или действий **злоумышленников** (хакер, инсайдер)	оперативное и полное **оповещение** субъектов ПД
нет **субъектов** из незащищенных групп населения	не было **жалоб**, претензий, исков в связи с инцидентом	**мониторинг** публикаций дампов и процесс их удаления
	~~ч. 1 ст. 13.11 не **применима**~~	комплекс **мер реагирования** и предотвращения инцидентов

Утечки ПД: процедура

72 часа с момента утечки

ВСЕ РАБОТНИКИ

незамедлительно

Совершен / выявлен инцидент с ПД

Уведомить ИТ и ИБ

ПРИМЕРЫ ИНЦИДЕНТА

- Увидели пост в ТГ-канале про утечку
- Случайно направили ПД не тому лицу ВНЕ КОМПАНИИ
- Увидели в открытом доступе клиентскую базу в Интернете
- Получили письмо с угрозами от хакеров

ИТ / ИБ

Проверить информа-цию и провести расследование

Нужно сообщить об инциденте, даже если:

(!) он произошел в отношении одного клиента/работника
(!) вы думаете, что это утечка, но точно не уверены
(!) вы думаете, что сообщение повлечет вашу ответственность за утечку (это не так)
(!) это выходной / праздник / отпуск, и вы не хотите беспокоить коллег (у РКН нет выходных)

ЮРИСТЫ

Привлечь DPO в случае установления инцидента с ПД

Поддержка в подготовке уведомления

МЕНЕДЖМЕНТ

Согласование подачи уведомления

Направление уведомления

Таймлайн

- фиксация результатов внутреннего расследования
- принятие решения о подаче уведомления (с ИТ и ИБ)
- **24 часа:** подача уведомления об инциденте в РКН
- **72 часа:** подача уведомления о результатах расследования в РКН
- дальнейшее взаимодействие с РКН

Уголовно-правовые риски

1

ЦЕЛЬ ОБРАБОТКИ	СУБЪЕКТЫ	ПОДЦЕЛИ ОБРАБОТКИ	ПЕРЕЧЕНЬ ПД	ИСТОЧНИК ПОЛУЧЕНИЯ
Проверка соискателей	• Соискатели • Родственники • Рекомендатели	• Проверка сведений ⚠ Дополнительные проверки безопасности и соответствия политикам • Оценка компетенций	• ФИО • Контакты ⚠ Сведения о судимости ⚠ Информация о поведении в социальных сетях	• Соискатели: направляемые резюме ⚠ Компании, проводящие проверку соискателей
Контроль за работниками	• Работники ⚠ Бывшие работники	• Меры ИБ ⚠ Анализ слитых БД • Защита имущества работников	• Фотоизображение ⚠ Геолокация ⚠ Содержимое переписки ⚠ Информация об используемых ИТ-сервисах	⚠ Работники: через ИТ-сервисы

2 **Каскадная ответственность** работников
регламентация периметра разрешенной обработки и зона ответственности

3 **Чистота получаемых ПД** от партнеров
через заверения и гарантии в договорах

4 **План** действий
поддержка работников и единая позиция

Проверить privacy-виктимность [1]

Локализация и трансгран

Метрики и аналитика

Политика обработки

Основания обработки

Информи-рование, DSR

Проверить privacy-виктимность [2]

Библиотека уязвимостей (частые примеры)

КРИТИЧНОСТЬ

Локализация и трансгран	Хостинг БД сайта вне РФ (IP-адрес)	Сбор ПД через зарубежные сервисы (опросы, капча)	В Политике нет трансграничной передачи ПД	Неуведомление РКН о трансграничной передаче ПД
Метрики и аналитика	Иностранные метрические сервисы (GA, FB пиксели)	В Политике нет деталей мониторинга	Нет cookie-баннера при первом касании	В cookie-баннере нет согласия
Политика обработки	Нет ссылки на каждой странице сайта, где собираются ПД	Разные объем и условия обработки ПД в Политике vs формах	Нет описания обработки для каждой цели, вкл. сроки	Нет описания порядка уничтожения ПД
Основания обработки	Избыточность ПД для заявленной цели	Нет учета и управления согласиями	Некорректные согласия	Нет согласия на распространение / ограничений
Информи-рование, DSR	Не исполнен запрос на доступ к ПД	Регистрация в реестре неактуальна и не соответствует сайтам	Нарушены сроки / порядок реагирования на запрос субъекта	Галочка есть, но нет текста согласия / информирования

Проверить privacy-виктимность [3]

Чек-лист

Контроль	Требование	Слож-ность внедре-ния	Матери-альность риска	Вероят ность обнару жения
• Уведомление в РКН	• Подано уведомление о намерении осуществлять обработку ПД	● ○ ○	● ○ ○	● ● ○
	• Подано уведомление о намерении осуществлять трансграничную передачу ПД	● ○ ○	● ○ ○	● ● ○
	• Данные в реестре операторов РКН актуализированы и соответствуют текущим процессам компании	● ○ ○	● ○ ○	● ● ○
• Обработка cookie-файлов				
• Локализация ПД	• База данных сайта размещена на российских серверах	● ● ●	● ● ●	● ● ○
	• Не используются зарубежные сервисы, которые не локализованы (reCaptcha, сервисы для опросов и др.)	● ● ○	● ● ●	● ● ●
	• Не используются зарубежные сервисы веб-аналитики (Google Analytics,Facebook*-пиксели и др.)	● ● ○	● ● ●	● ● ●
• Политика				
• Правовые основания обработки				
• Реклама				
• Реагирование на запросы				
• Рекомендательные технологии				
• Авторизация пользователей				
• Обязанности организатора распространения информации				
• Распространение ПД	• Если на сайте публикуются ПД, то у субъектов получены согласия на распространение	● ● ○	● ● ○	● ● ○
	• Если собираются согласия на распространение, то на сайте опубликованы запреты и ограничения на дальнейшую обработку опубликованных ПД	● ● ○	● ● ○	● ● ○
• Контент-комплаенс				

План действий

Группа мер		Содержание	Ответственные
Защита данных	🔥🔥	Приоритезировать защиту ИТ-систем (объем данных / спец. категории ПД и несовершеннолетние)	ИБ
	🔥	Оценить внешние ИТ-системы на предмет критичности, принять необходимые меры в отношениях с провайдерами	
	🔥	Обеспечить защищенность данных в ИТ-системах (внешний аудит и пентесты ежегодно, актуализация мер ИБ)	
	🔥🔥	Подготовить акты оценки эффективности СЗИ (самостоятельно или провести аудит ИБ)	
	🔥	Оценить расходы на ИБ — ФОТ компании не учитывается, только расходы на лицензиата ФСТЭК или ФСБ.	
Комплаенс	🔥🔥	Оценить изменения закона и составить план компенсирующих мероприятий	DPO Юристы ИБ
	🔥	Подготовить рассылку для работников с ключевыми принципами (контакты на случай утечки, примеры утечек или атак)	
	🔥	Провести ежегодную комплаенс-проверку и сформировать заключение	
	🔥🔥	Подготовить иные необходимые комплаенс-артефакты (журналы тренингов, проверок систем и контрагентов, сбор и актуализация перечня ПД, акты уничтожения и др. по чек-листу Comply)	
	🔥	Ужесточить контроль за заключением договоров с подрядчиками, в рамках которых есть передача (доступ) ПД	
	🔥🔥	Подготовить программу повышения осведомленности работников о требованиях	
	🔥	Внедрить zero-risk подход для новых процессов по сбору или получению ПД с предварительной проверкой комплаенса	
Реагирование на инцидент	🔥	Актуализировать план действий в случае инцидента (в каких случаях уведомляем гос. органы, кто / в какие сроки / что должен сделать, коммуникации с субъектами ПД, расследование, предпринимаемые меры и др.)	ИБ DPO Юристы
	🔥	Провести учения по реагированию на инциденты ИБ (смоделировать утечку)	

4

Законность обработки

Требования к обработке – «чек-лист»

Основание обработки

На каком основании обрабатываем?

Условия передачи ПД

Участвуют ли в обработке 3-и лица? Есть ли необходимые договоры?

Сроки обработки

Срок обработки ПД разумный и обоснованный?

Меры защиты ПД

Приняты ли меры защиты ПД, ограничен ли доступ к ним?

Минимизация ПД

Не обрабатываем ли больше, чем требуется?

Локализация ПД

Сохранены ли ПД первично на сервере в РФ?

Основания обработки ПД

Согласие субъекта

Законный интерес оператора и третьих лиц

Заключение и исполнение договора с субъектом

Исполнение обязанностей в соответствии с законом

Защита жизненно важных интересов субъекта

Публичные интересы, государственные функции

Согласие на обработку ПД

Согласие субъекта

Нужно ли брать согласие?

- **согласие работника**
- **реклама, продвижение** путем прямых контактов (смс, email, звонки и т.д.)
- **распространение ПД** в публичных источниках
- **нет другого** основания

Можем ли обойтись без него?

- договор с субъектом
- требования закона
- законный интерес
- другие основания

Правомерна публикация ПД на основании закона без согласия – дело Арсенала

В какой форме?

- простая форма или
- строгая письменная форма:
  - передача ПД **работников**
  - обработка **специальных** категорий ПД
  - обработка **биометрии**

Виды согласий

Простая форма

Оператор обязан **подтвердить факт получения согласия**. Способ получения согласия оператор может выбирать самостоятельно, но обязан **сохранять доказательства (логи)** получения согласия

- устно (аудиозапись разговора)
- «галочкой» на сайте
- смс, email, через мессенджеры

Письменная форма

Для письменного согласия установлены **строгие требования**, несоблюдение которых фактически равнозначно отсутствию согласия

- на бумажном носителе
- с использованием ЭП / особенности подписания в КЭДО

Согласие должно быть:

- ✓ **Свободным**
  Нельзя включать в текст договора, принуждать к даче согласия
- ✓ **Явно выраженным**
  Молчание ≠ согласие

Риски из согласий на рекламу

Ниже представлена положительная и негативная практика применения того или иного подхода

КОНВЕРСИЯ

РИСКИ

До **1 млн**. руб. за **каждое** производство

Репутационные издержки

OPT-IN

Собирается отдельно от других согласий и является необязательным

OPT-OUT

Галочка в согласии предпроставлена или имеется чек-бокс "не согласен на получение рекламы" с заранее не проставленной галочкой

HARD OPT-OUT

Нет отдельного чек-бокса для рекламного согласия, отказаться от рекламы невозможно до заключения договора / регистрации

НЕТ РИСКА

НИЖЕ СРЕДНЕГО И СРЕДНИЙ

Постановление Девятого АС Постановление АС Московского округа Решение АС г. Москвы, Определение Самарского УФАС Решение Башкортостанского УФАС

ВЫШЕ СРЕДНЕГО И ВЫСОКИЙ

Постановление АС Московского округа Предписание Московского УФАС Предупреждение Санкт-Петербургского УФАС Решение комиссии УФАС по Москве Постановление АС Московского округа

comply.ru | t.me/comply_ru | info@comply.ru

Comply.

Атрибуты для подтверждения рекламных согласий

Бумажное согласие

Копия печатной формы с данными:

- номер телефона/адрес электронной почты
- галочка с согласием
- подпись и дата подписания

Согласие на сайте

Лог-файлы или записи электронных журналов с регистрацией данных:

- номер телефона/адрес электронной почты
- дата и время согласия
- IP-адрес
- ConsentID / ссылка на форму

Согласие в колл-центре

Запись разговора с данными:

- подтверждение дачи согласия в записи
- номер телефона
- дата и время звонка / согласия
- подтверждать принадлежность номера телефона не требуется (Постановление 20 ААС А62-7498/2022)

Идентификация НЕ обязательна… пока

- решение АС Смоленской области от 17.03.2023 № А62-8361/2022
- постановление АС Московского округа от 05.05.2021 № А41-51750/2020

РИСКИ

- Общий лог действий
- Логгер на согласия
- История в CRM / C-M
- CJM / процесс
- Не хранить ничего

Основания, кроме согласий [1]

Заключение и исполнение договора с субъектом

Условия использования	Примеры
• ПД строго **необходимы** для заключения/исполнения договора • Субъект ПД – сторона, выгодоприобретатель или поручитель • Договор **не содержит** положения, ограничивающие права и свободы субъекта ПД (практика)	• Получение от соискателей минимально необходимого набора данных для отбора • Обработка данных посетителя сайта / пользователя мобильного приложения • Обработка данных родственников работников для ДМС

Ст. 16 ЗоЗПП: продавец не вправе отказывать потребителю в заключении, исполнении, изменении или расторжении договора с потребителем в связи с отказом потребителя предоставить персональные данные

Основания, кроме согласий [2]

Исполнение обязанностей в соответствии с законом

Условия использования	Примеры
• Нет требований получить согласие • ПД строго необходимы для исполнения обязанности / требования закона	• Предоставление бухгалтерской и налоговой отчетности по НК РФ и Закону о бух. учете • Получение документов при приёме соискателей по ТК РФ • Проверка контрагентов по НК РФ • Обработка ПД представителя контрагента

Примеры требований закона

Федеральный закон № 115-ФЗ «О противодействии легализации (отмыванию) доходов...»	обязывает банки идентифицировать клиентов, хранить в течение 5 лет и передавать ПД в Росфинмониторинг.
Федеральный закон № 395-1 "О банках и банковской деятельности"	обязывает банки сохранять банковскую тайну, устанавливает порядок раскрытия информации по запросам государственных органов.
Федеральный закон № 161-ФЗ «О национальной платёжной системе»	регулирует порядок обработки ПД в рамках платёжных операций и взаимодействия с платёжными системами.
Федеральный закон № 218-ФЗ «О кредитных историях»	регулирует порядок предоставления/получения сведений из БКИ
Положение Банка России № 851-П	устанавливает требования по обеспечению защиты информации с целью противодействия переводам денежных средств без согласия клиента

Итого

	Согласие	Договор	Закон	Интерес
Периметр обработки	🟢 🟢 🟢	🟡 🟡 ⚪	🔴 ⚪ ⚪	🔴 ⚪ ⚪
Срок обработки	🟡 🟡 ⚪	🟡 🟡 ⚪	🟡 🟡 ⚪	🟡 🟡 ⚪
Права субъекта	🔴 ⚪ ⚪	🟡 🟡 ⚪	🟢 🟢 🟢	🟡 🟡 ⚪
CJM и иная обременительность	🔴 ⚪ ⚪	🟡 🟡 ⚪	🟢 🟢 🟢	🟢 🟢 🟢
Надежность / Токсичность	🟡 🟡 ⚪	🟡 🟡 ⚪	🟢 🟢 🟢	🔴 ⚪ ⚪
Изменение условий оператором	🔴 ⚪ ⚪	🟡 🟡 ⚪	🔴 ⚪ ⚪	🟢 🟢 🟢

Ст. 16 ЗоЗПП: продавец не вправе отказывать потребителю в заключении, исполнении, изменении или расторжении договора с потребителем в связи с отказом потребителя предоставить персональные данные

5

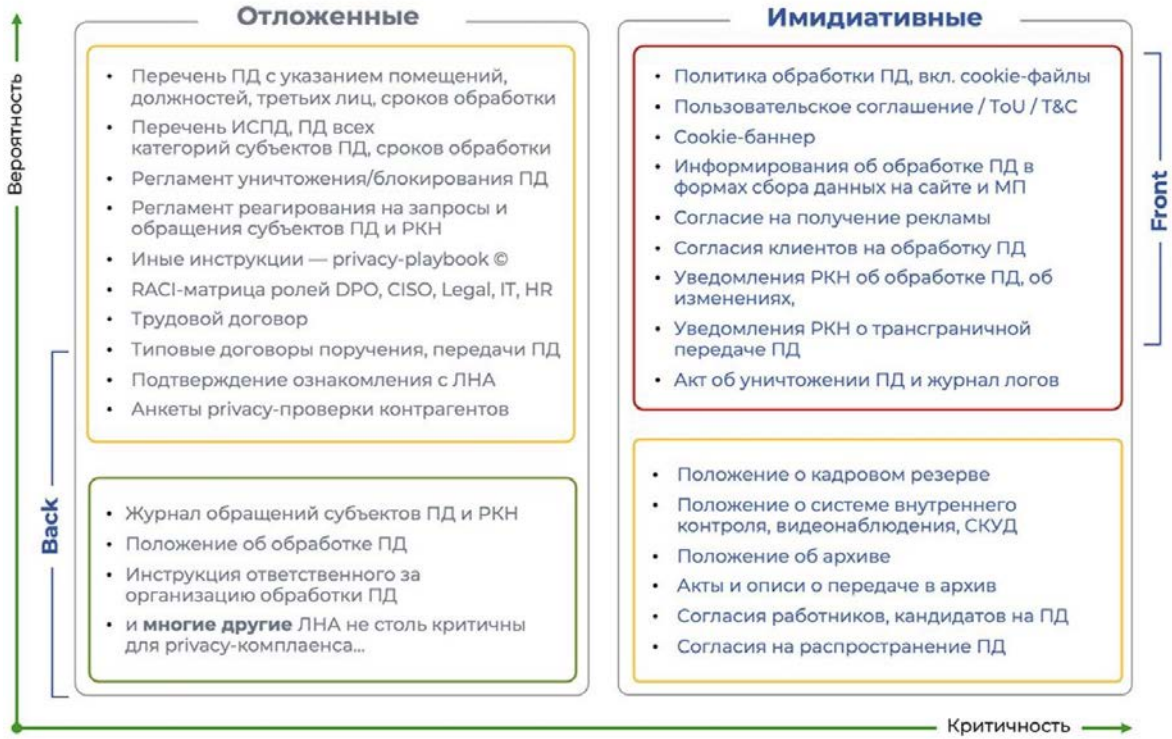
Контроли и процедуры

- Бумажный комплаенс
- RoPA
- Контроль изменений
- Передача ПД
- Сроки и объем обработки ПД
- Прекращение обработки ПД
- Запросы субъектов

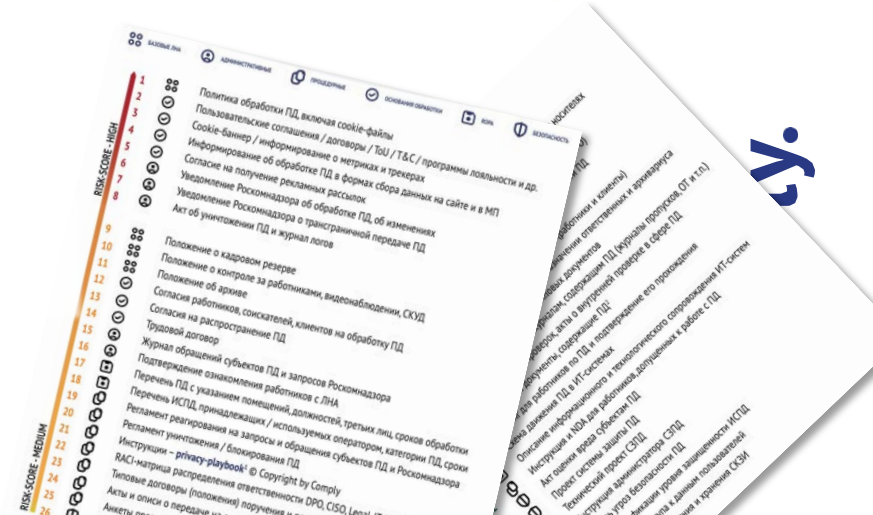
Бумажный комплаенс

Не все документы одинаково полезны. А «незаменимое» Положение о ПД заслуживает самое скромное внимание.

- «Документарные» риски носят отсроченный характер. **Неотложные** риски связаны с дефектами оснований обработки ПД или отсутствием Политики.
- **Сложность и трудоемкость** их подготовки. Например, сделать акты об уничтожении ПД или пересобрать согласия оперативно не выйдет, а Положение просто сделать быстро.
- Влияние на **privacy-виктимность**. Очевидность отсутствия или дефектов в документах.



Список TOP-50
privacy-документов



Перечень обработки ПД (RoPA) [1]

Образец Перечня

Требования закона с 1 сентября 2022

Цель обработки

- категории ПД = ФИО, паспортные данные, дата рождения, ID, ...
- категории субъектов ПД = работники, клиенты, представители контрагентов, ...
- способы обработки ПД = автоматизированная / смешанная + перечень действий (забыли?)
- сроки обработки ПД = конкретный срок: в течение 5 лет (с даты окончания договора)
- основания обработки ПД = согласие, исполнение договора, исполнение закона, ...
- порядок уничтожения ПД = удаление, сжигание, стирание, вымарывание, ...

- места хранения ПД = местоположение серверов, содержащих базы ПД
- ИТ-системы = названия / ссылки на перечень ИТ-систем, обрабатывающих ПД
- третьи лица = названия / ссылки на перечень внешних обработчиков / операторов ПД

⚠ Гигиенический минимум для обновленного уведомления РКН и **privacy-контролей**

Comply.

Перечень обработки ПД (RoPA) [2]

Как собрать и сопровождать?

1 Провести аудит процессов и инвентаризацию ПД	• интервью с бизнес-подразделениями • опросники для самозаполнения
2 Определить форму ведения реестра	• таблица в Excel или документ в Word • интерактивные таблицы в Notion / AirTable • специальные решения
3 Определить ответственного за ведение реестра	• DPO • иные внутренние подразделения / privacy-чемпионы • аутсорсинг консультантам
4 Определить порядок обновления реестра	• плановые проверки • бриф-аудиты • репортинг DPO о всех изменениях (privacy-культура)

Comply.

Изменения процессов: процедура

Изменения процессов: ключевые элементы

- Обучение / RACI / Privacy-playbook (понятные инструкции и сроки, триггеры и красные флаги)
- Privacy-чемпионы и мотивация
- Типовые формы для оценки новой системы, контрагента вкл. privacy-аспекты
- Актуализация RoPA
- Выборочный контроль DPO

Comply.

Передача ПД: статус

Оператор	Обработчик
• Определяет: o цели обработки o состав ПД o действия (операции) с ПД • Обеспечивает законность обработки	• Обрабатывает ПД по поручению / от имени оператора • Не имеет своих целей обработки ПД • Может определять только технические средства обработки ПД
• Ответственность **перед субъектами и Роскомнадзором**, в т.ч. за нарушения обработчика	• Ответственность **только перед оператором** (кроме иностранных обработчиков) **по договору**

Передача ПД: статус

Ответственность за обработчика
Фиксация в согласиях, Политике, реестрах

Оператор – Оператор	Оператор – Обработчик
РЖД и Яндекс Go	Аутсорсинг ИТ-поддержки
Работники клиентов / контрагентов	Travel-агентство
ЧОП	Хостинг-провайдер
Банк и страховая для работников	PR/маркетинговое агентство
Внешние аудиторы	
Лицензированные обучающие организации	

Передача ПД: требования к договорам

Оператор – Оператор

152-ФЗ не устанавливает требований, НО на практике **необходимо** включать:

- обязанности по **защите ПД** и
- **перечень ПД**

Не всегда инспектор Роскомнадзора понимает разницу двух моделей передачи данных.

Кроме этого, **рекомендуем** включать обязанности другой стороны по:

- содействию при запросах субъектов
- содействию при инцидентах с ПД / ИБ
- гарантии правового основания обработки и передачи ПД
- соблюдению конфиденциальности при передаче

Оператор – Обработчик

Ч. 3 ст. 6 152-ФЗ устанавливает **требования** к поручению:

- **перечень ПД** [эксцесс исполнителя]
- **операции по обработке ПД**
- цели обработки ПД
- обязанности обработчика:
  - соблюдать принципы и правила обработки ПД, и **конфиденциальность** и безопасность ПД, включая меры по **ч. 5 ст. 18, ст.ст. 18.1 и 19**
  - **предоставлять доказательства их соблюдения**
  - **уведомление оператора об инцидентах с ПД и сроки такого уведомления**
  - особенности обработки ПД на мат. носителях
  - уничтожать и подтвердить уничтожение ПД по запросу оператора

новое требование с 01.09.2022 / 01.03.2023

Передача ПД: процедура контрактования

В случае передачи исключительно **контактных данных** и **ПД подписантов** работник включает в договор **общую оговорку о ПД**

Передача ПД: трансграничная передача

«Адекватные» страны

- Страны-участницы Конвенции Совета Европы № 108 (в т.ч. Грузия и Армения)
- Страны из списка Роскомнадзора


ЕС


Китай


Индия


Бразилия


ЮАР

«Неадекватные» страны

- Все остальные страны


США


ОАЭ

Уведомить Роскомнадзор ДО трансграничной передачи

Применяется с 1 марта 2023

Можно передавать с момента уведомления Роскомнадзора

Если запрета или ограничений нет в течение 10 дней, то **можно** передавать

Comply.

Передача ПД: трансграничная передача

Случаи запрета:

представление государственных органов в Роскомнадзор

получатели ПД не принимают меры по защите передаваемых ПД, не определены условия прекращения их обработки

получатель ПД является запрещенной организацией на территории РФ или признан нежелательным в РФ

трансграничная передача и дальнейшая обработка переданных ПД не совместима с целями сбора ПД

трансграничная передача ПД осуществляется без законного основания, предусмотренного ст. 6 Закона о ПД

Основания для ограничения:

представление государственных органов в Роскомнадзор

содержание и объем ПД, планируемых к трансграничной передаче, не соответствуют цели трансграничной передачи

категории субъектов ПД не соответствуют цели трансграничной передачи

Решение об ограничении должно содержать **уточненный РКН перечень** целей трансграничной передачи ПД, категорий субъектов ПД, содержания и объема ПД, планируемых к трансграничной передаче

⚠ Запрет действует на всю трансграничную передачу, указанную в уведомлении

⚠ Ограничение действует только в той части, которая НЕ соответствует требованиям

Локализация ПД

Локализация

Сбор ПД должен осуществляться с использованием баз данных (БД) на серверах в РФ

В ходе проверок Роскомнадзор требует **предоставления логов из ИТ-систем**, подтверждающих сохранение ПД в локальных БД

- Передача **третьим лицам** возможна только после обеспечения локализации в РФ
- Передача в **иностранную БД / облачное хранилище** одного оператора возможна после записи в локальной (РФ) базе
- Изменение, копирование, систематизация ПД в иностранной БД возможны только **после отражения таких изменений в локальной БД**

Штрафы за нарушение

До 18 млн. руб.
для компании

До 800 тысяч руб.
для должностного лица компании

Comply.

Срок и объем обработки ПД

Сроки обработки ПД должны быть ограничены достижением цели обработки!

Компания определяет целевые сроки обработки для каждого бизнес-процесса

Компания выполнила цель обработки, прошел целевой срок обработки

Ответственные работники прекращают обработку ПД (см. следующий слайд)

Примеры целевых сроков*

- Резюме и анкеты соискателя – до 12 месяцев с даты подачи резюме
- Кадровые документы – 5 лет после прекращения трудовых отношений
- Записи звонков в колл-центр – до 6 месяцев с даты обращения

* Целевые сроки определяются в Компании в т.ч. с учетом устоявшихся подходов рынка и регуляторов

Применимо к ПД в любом формате: ИТ-системы, сетевые диски, бумага и т.д.

Прекращение обработки ПД [1]

- Для документов, которые требуется передавать в архив
- Внутренний формализованный архив или во внешнюю специализированную организацию
- Требования 152-ФЗ не применяются к хранению, комплектованию, учету и использованию архивных документов, содержащих ПД
- Обязательно подтверждается актом о передаче на архивное хранение

- Пока не допускается для коммерческих организаций
- Не прекращает действие 152-ФЗ

- Для документов, которые не требуется передавать в архив
- Способом, не позволяющим восстановить ПД (удаление из ИТ-систем / шредирование и т.д.)
- Обязательно подтверждается актом и выпиской из лог-файлов по утвержденной форме

Прекращение обработки ПД [4]

Уничтожение ПД подтверждается актом об уничтожении ПД и/или выгрузкой из журнала

Приказ РКН № 179 также требует указывать в акте:

- ФИО субъектов ПД и
- категории ПД

Необходимость прекратить обработку ПД

→ Уничтожение

в т.ч. документы по соискателям, карточки клиентов и контрагентов

Акт [номер] от [дата]

г. Москва

Оператор: [указать]

Адрес: [указать]

Настоящим актом фиксируется уничтожение персональных данных, обрабатываемых Компанией, за период [указать период]:

Бизнес-процесс	Отдел(ы)	Информационные системы	Материальные носители	Причина уничтожения	Способ уничтожения	Дата уничтожения
[указать из Перечня ПД]	*[указать из Перечня ПД]*	*[указать из Перечня ПД]*	*[указать из Перечня ПД]*	*[истечение срока обработки, достижение цели обработки, запрос субъекта, требование Роскомнадзора]*	*[путем измельчения (шредер), удаление из информационных систем (стирание информации с накопителей данных)]*	*[указать]*

Ответственный за организацию обработки персональных данных
[необходимо указать]

Уничтожение ПД: процедура

Рутинное уничтожение

Владелец бизнес-процесса, руководствуясь **инструкцией** DPO и **RoPA** по своим внутренним правилам:

- Уничтожают ПД
- Составляют акт об уничтожении
- Направляют акт DPO на подписание

Данная процедура производится **один раз в 6 месяцев**. ПД блокируются до истечения указанного срока

Уничтожение по запросу

В случае если DPO получает запрос субъекта или иное требование, влекущее за собой немедленное уничтожение ПД, то:

- DPO направляет запрос владельцам бизнес-процесса о необходимости уничтожения ПД
- Владелец бизнес-процесса удаляет ПД, составляет акт об уничтожении и направляет его DPO для заверения

Внедрение **автоматизированных** протоколов **уничтожения** ПД и **генерации** актов / журналов в системах

Запросы субъектов ПД (DSR) [1]

10 рабочих дней или иной срок

Запрос

- по e-mail
- по телефону
- устно при личном визите
- по SMS, в мессенджерах и т.д.
- от самого субъекта или представителя

Проверка

- достаточно e-mail, телефона или иного ID, субъекта в системе
- паспортные данные могут запрашиваться в исключительных случаях — например, запрос на доступ к ПД
- проверка полномочий представителя

Реализация

- направление ответа субъекту — в любом случае, даже если это отказ
- ответ в той же форме, в которой направлен запрос


Отзыв согласия

Блокировка, возражение


Доступ к ПД


Удаление


Изменение

Теперь субъекту нужно рассказывать о мерах безопасности при обработке ПД

Запросы субъектов ПД (DSR) [2]

ТЕМА ЗАПРОСА	ДЕЙСТВИЯ	СРОК ПРЕДОСТАВЛЕНИЯ ОТВЕТА
Ознакомление с ПД	Подтверждение обработки ПД	10 рабочих дней
	Отказ подтверждения обработки ПД	
Изменение / уточнение	Изменение ПД	7 рабочих дней
	Отказ в уточнении ПД	30 дней
Уничтожение	Уничтожение ПД	10 рабочих дней
	Отказ в уничтожении ПД	30 дней
Отзыв согласия на обработку ПД	Прекращение обработки и уничтожение ПД	30 дней, если иное не предусмотрено договором
	Отказ в прекращении обработки и уничтожении ПД	
Отзыв согласия на рекламу	Отписка от всех рассылок и иных маркетинговых активностей	1-3 дня
Неправомерность обработки ПД	Прекращение обработки ПД	3 рабочих дня
	Уничтожение ПД	
Прекращение обработки	Прекращение обработки ПД	10 рабочих дней
	Отказ в прекращении обработки ПД	
Запросы РКН	Предоставление информации	10 рабочих дней

Privacy playbook + RACI

ПРОСТЫЕ ГАЙДЫ:

- Риски перманентно увеличиваются
- Количество требуемых контролей растет
- DPO требуется поддержка – 1 линия

- изменение процессов обработки ПД
- запрос субъекта или РКН
- инциденты / утечки ПД
- привлечение нового подрядчика
- уничтожение ПД

- Сроки / SLA
- Цепочки действий
- Ответственные

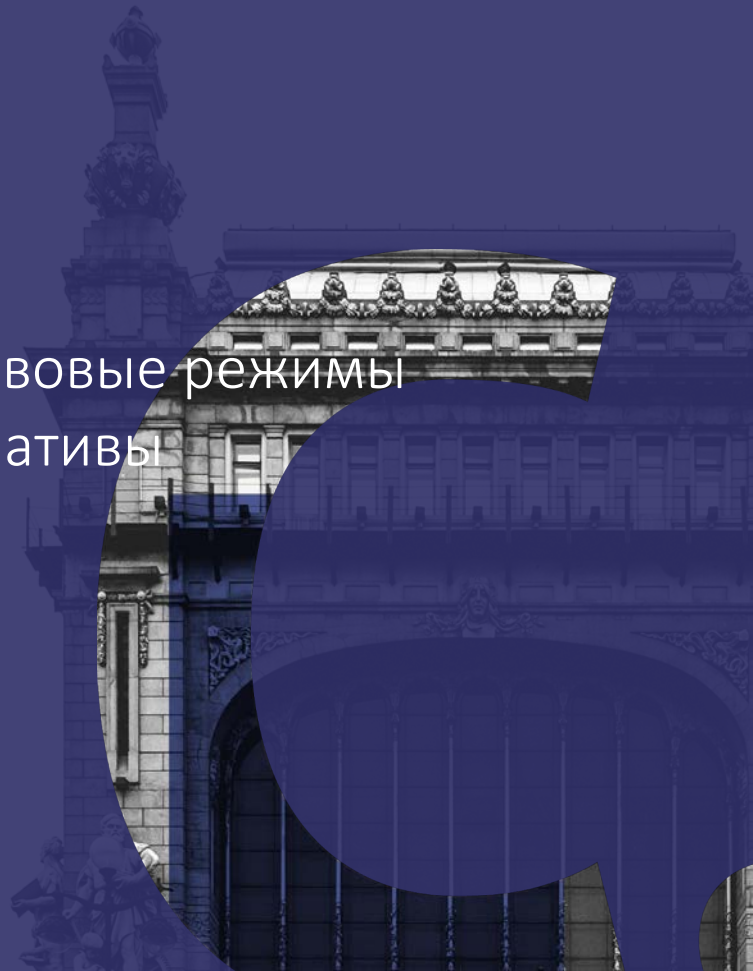
comply.ru | t.me/comply_ru | info@comply.ru

Comply.

6

Privacy & AI

- дата-национализация
- экспериментальные правовые режимы
- законодательные инициативы



Чем рискуем?

1. Обработка / передача без надлежащего законного основания
2. Дополнительная точка утечки данных
3. Трансграничная передача ПД в (не-)адекват и локализация
4. Нарушение соглашений с коммерческими клиентами
5. Непрозрачность обработки для субъекта
6. Автоматизированное принятие решений

Comply.

🎯 Разбираемся с целью

Выясняем, что вообще за ассистент:

Какого рода ассистента хотят внедрить / какую продуктовую задачу он будет решать:

- саппорт-бот
- агент
- генератор
- расшифровка аудио
- иное?

Что на выходе получит пользователь:

- поддержку
- работу с данными в системе
- контент
- аналитику

Позиционирование и планы на развитие:

- часть продукта
- доп. сервис
- перепродажа
- чистый маркетинг

Инструменты:

- 💬 Интервью с продактами и разработчиками
-  DPIA-опросник
-  Макеты и документация

Comply.

🔍 Анализируем потоки данных

Проверяем, как он будет работать с данными:

К каким данным получит доступ ассистент:

- данные юзера
- содержимое системы
- только медиа
- ни к каким, только промпт

Какая квалификация этих данных:

- ПД
- не ПД, но конфиденциальные
- безопасные

На каких правовых основаниях обрабатываются данные:

- согласие пользователя
- общий договор на продукт
- отдельный договор на этот сервис
- ~~законный интерес~~

Инструменты:

- 💬 Интервью с продактами и разработчиками
-  DPIA-опросник
-  Макеты и документация

Comply.

🔎 Анализируем потоки данных

Проверяем, как он будет работать с данными:

Как организовано управление доступом:

- global consent
- точечная передача конкретных данных
- возможности юзера ограничить доступ

Генерирует ли ассистент дополнительные данные / информацию:

- да — ПД
- да — не ПД, но КИ
- только медиа
- ничего

Как будет храниться и использоваться информация:

- переиспользование клиентских данных
- хранение в продуктовой БД
- отдельное хранилище / компонент

Инструменты:

- 💬 Интервью с продактами и разработчиками
-  DPIA-опросник
-  Макеты и документация

Comply.

🔎 Смотрим на нейросеть

Изучаем, какой сервис ляжет в основу:

Что за сервис будет использоваться:

иностранный SaaS	российский SaaS	локальная модель
• OpenAI • Claude • Gemini • Grok • Perplexity • DeepSeek • Deepgram	• Yandex AI Studio • GigaChat • T-Pro AI • Cotype	• Llama • QWen • Gemma • GPT-OSS

Comply.

🔎 Смотрим на нейросеть

Если иностранный SaaS:

В какой конкретно юрисдикции находятся сервера:

- ЕС
- США
- Китай
- РФ

Как платится подписка:

- корпоративный аккаунт = enterprise подписка
- чей-то личный аккаунт = базовая подписка

Что по обвязке:

- распределение ролей
- обязательства по конфиденциальности
- распределение прав на результаты

Сервис	Возможность размещения в ЕС
OpenAI	Да — есть возможность «Europe»
Anthropic Claude	Да — инфраструктура Europe
Google Gemini	Да — выбор «eu» мульти-регион
DeepSeek (via Perplexity)	Частично — US/EU дата-центры
Grok	Не ясно
Perplexity AI	Частично — ЕС/US

Comply.

🔎 Смотрим на нейросеть

Если российский SaaS:

Что по обвязке:

есть ли поручение на обработку ПД	обязательства по конфиденциальности	распределение прав на результаты

Comply.

🔎 Смотрим на нейросеть

Если локал:

Где будет хоститься:

- свой ЦОД (малореалистично)
- внешний ЦОД

Какие лицензионные ограничения:

- можно ли использовать в своем продукте

Comply.

Придумываем компенсирующие меры

Закрываем риски функционально и документально:

закрываем ПД через обезличивание	даем доступ только к числовой статистике	даем юзеру возможность самостоятельно решать
ищем российские аналоги	переносим модель на локал	выбираем регион хостинга
заключаем enterprise-соглашение	по возможности — заключаем поручение по своей форме	
прорабатываем transparency для юзера	заключаем отдельные соглашения / инструкции с пользователями на этот сервис	
даем возможность юзеру принести свой API-ключ		

Comply.

Comply.

comply.ru
t.me/comply_ru
info@comply.ru

ООО «Комплай»

Россия
ОГРН 1207800126742 | ИНН 7811751473
Санкт-Петербург, 193231, ул. Чудновского, д. 19

Армения
Рег. № 286.110.1233573 | ИНН 02861614
Ереван, 0023, пр. Аршакуняц, д. 4