



SmartKЭДО

КЭДО

Персональные данные в КЭДО:

что нужно знать
кадровику в 2025



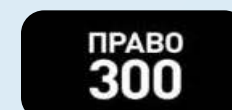


 @saiganov

 sergei@comply.ru

Сергей Сайганов

CEO **SmartKЭДО**,
юрист и эксперт по защите данных

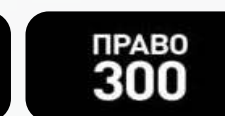


Более 10 лет проектного и юридического опыта в сфере технологий и информационной безопасности.

До учреждения Comply получил опыт в Group-IB и PwC. Участвовал в проектах по защите интеллектуальной собственности, регулированию работы с данными и отраслевому регулированию в сфере ИТ. Представлял интересы компаний при проверках регуляторов и в суде. Среди клиентов – Mercedes-Benz Rus, Melon Fashion Group, Акрихин, Calzedonia, HF Labs. Состоит в рабочих группах Роскомнадзора и законопроектных институтов, отраслевых ассоциаций. Отмечен российскими юридическими рейтингами Pravo.ru-300 и Коммерсантъ, лауреат премии «Privacy-консультант года», член RPPA.

Часть экосистемы
юридической фирмы **Comply**.

TOP-tier рейтинга Право.Ру-300 в номинации
Защита персональных данных, лучшая
консалтинговая фирма в области цифрового права



 **SmartKЭДО**

Система кадрового ЭДО, построенная по
принципу **Compliance-First**. Создана
профессионалами для профессионалов

Переводим кадровые процессы в цифру с учетом
всех требований законодательства

Высвобождаем время на развитие компании, HR-
бренда и бизнеса. Повышаем общую
цифровизацию и **оптимизируем процессы** для
экономии денег компании

Регулирование



⚖️ Федеральный закон № 152-ФЗ "О персональных данных"

⚖️ ст. 88 Трудового кодекса

- Существует довольно обширная нормативная база при регулировании ПД, включающая в себя в т.ч. большое кол-во подзаконных актов РКН, Минцифры, ФСТЭК и ФСБ
- Однако далеко не все требования прямо применимы к КЭДО и кадрам
- Ключевые требования, которые разберем далее:

Требования

Пояснение

правовое основание обработки ПД

= что позволяет компании обрабатывать ПД сотрудника

сроки обработки и прекращение обработки ПД

= сколько компания обрабатывает ПД, как контролирует и как перестает

урегулирование отношений с третьими лицами по ПД

= как выстроены отношения с подрядчиками при обработке ПД

обеспечение безопасности ПД

= что компания предпринимает при защите ПД

Правовые основания



⚖ ст. 6 152-ФЗ

Закон о ПД предусматривает целый ассортимент возможных правовых оснований, каждое из которых, в теории — подходит для обработки ПД сотрудников:

исполнение требований законодательства

заключение и исполнение договора с субъектом

обеспечение законных интересов оператора

согласие субъекта на обработку ПД

... а также ряд других, совсем неприменимых

Но есть одно большое
⚖ НО — в виде позиции
регулятора!



Согласие сотрудника



Роскомнадзор:

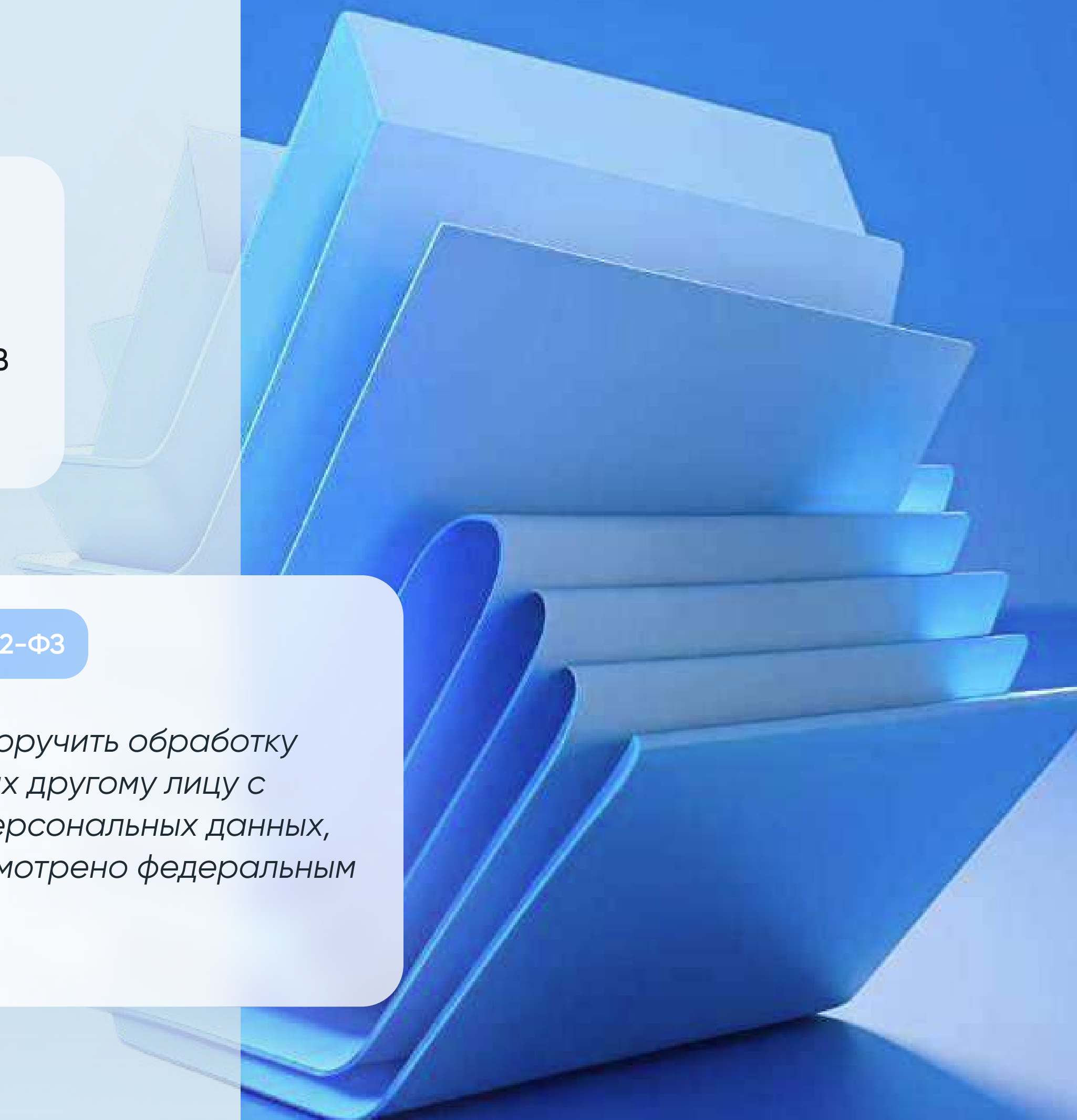
Необходимое правовое основание для обработки ПД сотрудников
— **письменное согласие** в соответствии с законодательством

⚖ абз. 2 ст. 88 ТК РФ

«... не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами»

⚖ ч. 3 ст. 6 Закона № 152-ФЗ

«Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом...»



Состав согласия



⚖ ст. 9 Закона № 152-ФЗ

Требование

«Согласие на обработку персональных данных должно быть:

- конкретным,
- предметным,
- информированным,
- сознательным и
- однозначным»

Пояснения

= раскройте все параметры обработки ПД:

цель обработки ПД

перечень обрабатываемых ПД для этой цели

срок обработки ПД

допустимые операции с ПД

третьи лица, которые могут участвовать в обработке ПД

Содержание согласия



Идентификация субъекта:

- ФИО, адрес, паспортные данные.
- ~~Должность сотрудника или его номер телефона~~

Идентификация оператора: наименование работодателя, адрес регистрации, ИНН/ОГРН

Конкретная цель по принципу "одна цель — одно согласие":

- осуществление взаимодействия с работодателем посредством системы кадрового электронного документооборота
- ~~"исполнение требований законодательства"~~

Перечень обрабатываемых ПД: ФИО, адрес, паспортные данные, табельный номер, ...,
+ [иные сведения, содержащиеся в кадровых документах](#)

Перечень действий с ПД: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (~~распространение~~, предоставление, доступ), ~~обезличивание~~, блокирование, удаление, уничтожение

Идентификация "обработчика" - вендора КЭДО: наименование, адрес регистрации, ИНН/ОГРН

Срок обработки:

✓ **Можно:**

Конкретная дата

Конкретное событие — достижение цели (окончание трудовых отношений)

✗ **Нельзя:**

Бессрочное

Автоматическая пролонгация

Чрезмерно длительный срок (50 или 75 лет)

[Вебинар Роскомнадзора](#) «Изменения законодательства в сфере персональных данных, 29 марта 2022

Информационное письмо Роскомнадзора и Банка России о согласии заемщиков на обработку их персональных данных № 08ЛА-48666 / № ИН-06-59/57 от 29.07.2021,

Последствия несоблюдения формы согласия



SmartKЭДО

1. Предписание РКН устранить нарушения (= переподписать **все** согласия)

2. Административная ответственность:

☞ ч. 2–3 ст. 13.11 КоАП РФ

Ответственность:

для должностных лиц: первое — до 300 000 ₽,
повторное — до 500 000 ₽

для предпринимателей: до 1 000 000 ₽

для юридических лиц: первое — до 700 000 ₽,
повторное — до 1 500 000 ₽

Примеры нарушений:

несколько целей в согласии

бессрочное действие или неконкретный срок
(например, до момента отзыва)

отсутствие реквизитов обработчиков ПД по
поручению оператора

мы всегда разрабатываем
для наших клиентов
корректную форму согласия
в ходе внедрения

Пример согласия:



Сроки обработки ПД

⚖ ст. 5 152-ФЗ

Сроки обработки (вкл. хранение) ПД должны быть ограничены **минимально необходимыми** для достижения конкретной цели

Сроки должны быть определены на уровне локальных актов оператора (в т.ч. Реестра обрабатываемых ПД) и прямо указаны в согласии на обработку ПД

На практике РКН требует, чтобы сроки были конкретно определены оператором:

либо в **твердых числах** (5 лет, 10 лет и т.д.)

либо наступлением какого-то **конкретного события** (окончание трудового договора)

Обратные ситуации наказуемы — **не принимаются** формулировки:

- ~~"не ограничены"~~
- ~~"до момента отзыва"~~
- ~~"до достижения цели"~~
- ~~"в соответствии с законодательством"~~

Для корпоративных систем есть конкретная практика в рамках проверок РКН:

к обработке ПД работников в 1С ЗУП и др. кадровых системах:
не более 5 лет с даты увольнения

к обработке ПД соискателей:
не более 12 месяцев с даты предоставления согласия

Сроки обработки ПД



По истечению сроков нужно прекращать обработку ПД:

либо уничтожать ПД и составлять акт об уничтожении

либо — **архивировать ПД** надлежащим образом

⚖ Приказ Росархива № 236

⚖ Федеральный закон № 125-ФЗ “Об архивном деле”

В КЭДО практически никогда ПД не уничтожаются, т.к. они содержатся в кадровых документах, подлежащих долгосрочному хранению в течение 5 / 25 / 50 лет и т.д.

⚖ Но корректным прекращением обработки ПД архивация считается только при **правильной реализации архива** — как в SmartКЭДО:

настраиваемый контроль сроков хранения документов

автоматическое перемещение данных и документов сотрудника в течение 30 дней после увольнения в архив

изолированная архивная система, отделенная от оперативной, со своей системой авторизации и ролевой моделью

хранение всех метаданных документа и возможность экспорта в исходном виде

= так, как это сделано только у нас в



SmartКЭДО

Последствия несоблюдения сроков обработки



1. Предписание РКН устранить нарушения (= переделать системы и процессы в срок не более 3 месяцев)
2. **Административная ответственность**, т.к. обработка сверх срока = осуществляемая без законного основания:

⚖ ч. 1-2 ст. 13.11 КоАП РФ

Ответственность:

для должностных лиц: первое — до 100 000 ₽,
повторное — до 200 000 ₽

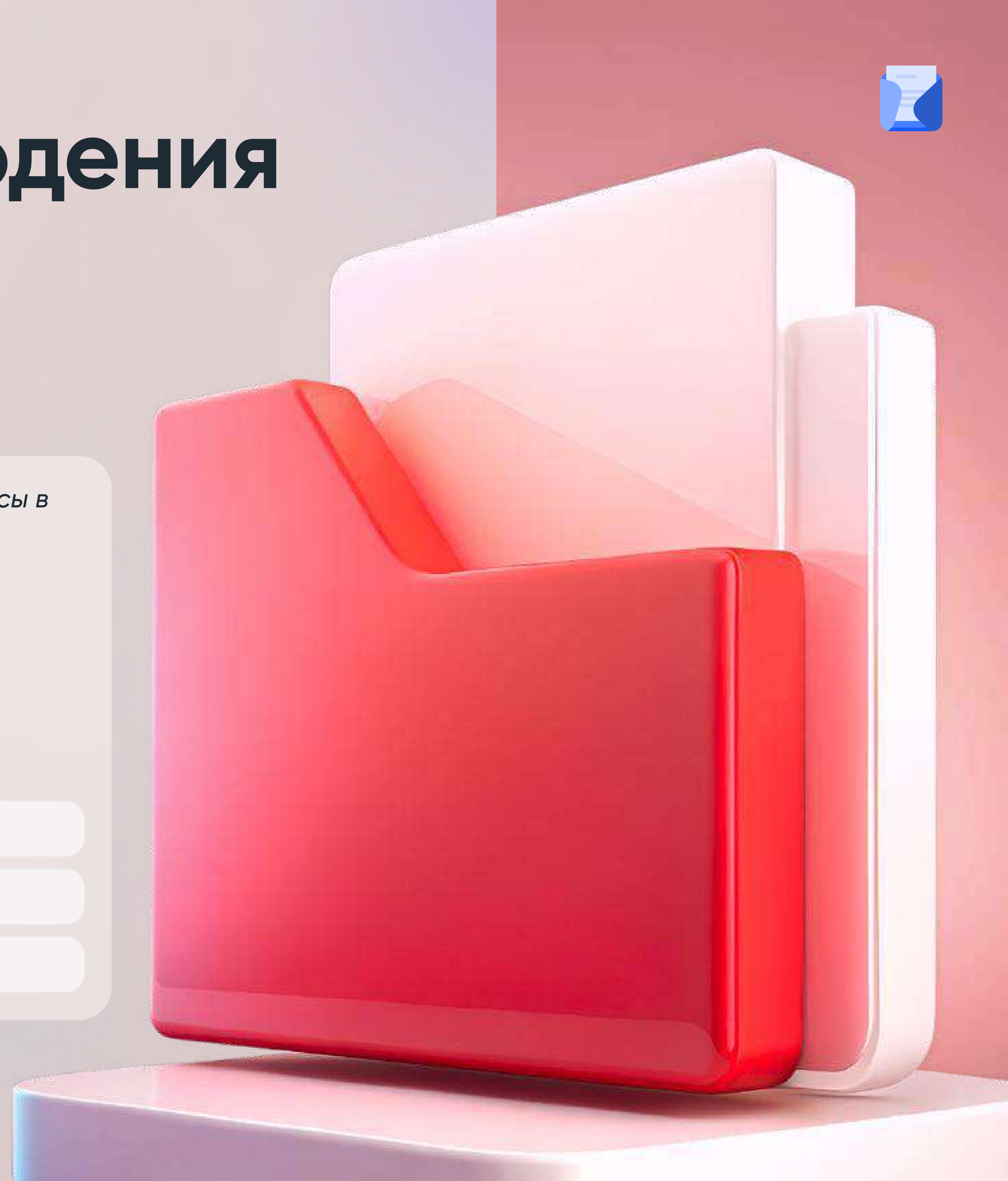
для юридических лиц: первое — до 300 000 ₽,
повторное — до 500 000 ₽

Примеры нарушений:

не определены сроки в локальных актах

не уничтожены ПД по истечению срока

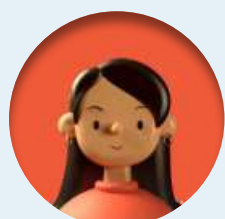
некорректно архивированы ПД



Отношения с третьими лицами

⚖️ ч. 3 ст. 6 152-ФЗ

Оператор вправе поручить обработку ПД третьему лицу на основании договора поручения



Компания



Вендор КЭДО

привлекает вендора КЭДО к обработке ПД на основании договора

является оператором ПД, определяет систему КЭДО, состав ПД, цели, сроки и способы обработки

полностью отвечает за обработку ПД перед законом и субъектами

получает и хранит ПД сотрудников при "облачном" хостинге системы КЭДО

имеет доступ к ПД в рамках техподдержки, если компания размещает КЭДО на своих серверах

отвечает перед оператором за допущенные нарушения в рамках договора поручения

Поручение на обработку ПД **обязательно** для включения в договор с вендором КЭДО

Требования к поручению



⚖ ч. 3 ст. 6 152-ФЗ

⚖ ст. 18.1-19 152-ФЗ

ОБЯЗАННОСТИ ОБРАБОТЧИКА

Соблюдение конфиденциальности и инструкций оператора

Перечисление мер по выполнению требований из ст. 18.1. Закона

Требования к безопасности из ст. 19 Закона

Предоставление оператору документов и информации, подтверждающих выполнение требований закона и поручения

Обеспечение локализации ПД на территории России при сборе данных

Уведомление оператора об утечке не позднее 24 часов после обнаружения

ПАРАМЕТРЫ ОБРАБОТКИ

Подробный перечень обрабатываемых ПД:

- ФИО, паспортные данные, номер телефона, ...
- *+ иные данные в составе кадровых документов*

Перечень действий с ПД:

- получение, хранение, систематизация, доступ, ...

Цель обработки:

- ~~исполнение договора~~ / ~~законодательства~~
- *обеспечение поддержки используемой системы КЭДО в соответствии с договором...*

 **SmartKЭДО**

**мы всегда заключаем
корректное поручение с
нашими клиентами**

Пример поручения:



Последствия некорректного поручения



1. Предписание РКН устранить нарушения (= *переподписать поручение*)
2. **Административная ответственность**, т.к. некорректное поручение обработки = обработка без законного основания:

⚖ ч. 1-2 ст. 13.11 КоАП РФ

Ответственность:

для должностных лиц: первое — до 100 000 ₽,
повторное — до 200 000 ₽

для юридических лиц: первое — до 300 000 ₽,
повторное — до 500 000 ₽

Примеры нарушений:

не определен состав ПД к обработке

не прописаны меры по обеспечению
безопасности

не заключено поручение вовсе

3. Потенциально — некорректно оформленный доступ подрядчика к ПД может быть признан **утечкой ПД по вине оператора**



Безопасность ПД

⚖ ст. 18.1 – 19 152-ФЗ

Оператор обязан обеспечивать безопасность всех обрабатываемых ПД

Эта обязанность распространяется также на все внешние системы, которыми пользуется оператор ПД, а также на всех обработчиков ПД по поручению оператора

Безопасность достигается двумя обязательными блоками работы

документальная — в формате принятия нужных ЛНА, актов и т.д.

и реальная — путем фактической настройки, тестирования и администрирования процессов защиты ПД в системах

Но в КЭДО компания редко может повлиять на реальную безопасность, т.к. владельцем, разработчиком и администратором системы обычно является вендор КЭДО, т.е. третье лицо — обработчик

Поэтому компаниям критично важно:

1. заключить корректное поручение
2. убедиться, что вендор КЭДО **знает и понимает**, как работать с ПД (что бывает не часто)

Последствия плохой безопасности ПД



1. Неминуемая утечка ПД

2. Административная ответственность — с мая 2025:

⚖ ч. 1-2 или 11-18 ст. 13.11 КоАП РФ

сценарий-лайт (до 1 000 субъектов):

для должностных лиц: первое — до 100 000 ₽,
повторное — до 200 000 ₽

для юридических лиц: первое — до 300 000 ₽,
повторное — до 500 000 ₽

сценарий-жесть (от 1 000 и более):

для должностных лиц: первое — 300 000–600 000 ₽,
повторное — 800 000–1 200 000 ₽

для юридических лиц: первое — 3 млн–15 млн ₽,
повторное — до 500 млн ₽ или 1-3% от оборота

3. Уголовная ответственность — уже сейчас:

- штраф до 300 000 ₽ или в размере годового дохода, либо
- принудительные работы до 4 лет, либо
- лишение свободы до 4 лет



Последствия плохой безопасности ПД

Новое: КоАП



Июнь 2025

не все изменения — только основное

Состав	Штраф для ЮЛ, руб.	Штраф для работника *
Утечка до 1k субъектов или неправомерная обработка	150 – 300k	50 – 100k
То же самое, но повторно	300 – 500k	100 – 200k
Неуведомление РКН об обработке или утечке ПД	300k – 3 млн	50k – 800k
Обработка ПД без письменного согласия (если нужно)	300k – 1.5 млн	300k – 500k
Утечка ПД 1k – 10k субъектов ПД и (или) x10 ID**	3 – 5 млн	200 – 400k
Утечка ПД 10k – 100k субъектов ПД и (или) x10 ID	5 – 10 млн	300 – 500k
Утечка ПД более 100k субъектов и (или) x10 ID	10 – 15 млн	400 – 600k
Повторная утечка, не включающая биометрию или специальные категории ПД	1 – 3% выручки за год	800 – 1,2 млн
Утечка, включающая ПД специальных категорий	10 – 15 млн	1 – 1,3 млн
Утечка, включающая биометрические ПД	15 – 20 млн	1,3 – 1,5 млн
Повторная утечка биометрии или спец. категорий ПД	1 – 3% выручки за год	1,5 – 2 млн

Утечка – неправомерная или случайная передача ПД (предоставление, распространение, доступ), повлекшая нарушение прав субъектов ПД.

Не является утечкой:

- НСД внутреннего пользователя к базе без копирования
- Случайное уничтожение базы внутренним пользователем
- Подозрительная активность пользователя системы

* ГД, рук-ли отделов, DPO могут быть привлечены к ответственности только за утечку ПД менее чем 1k субъектов (в т.ч. повторную).

1 / 40 случаев привлечение работника к ответственности за утечку.

** ID – уникальное обозначение сведений о физическом лице.

Запись выступления:



Comply.

Как обеспечивается безопасность у нас?



SmartKЭДО

мы точно знаем, как работать с ПД

являемся **частью экосистемы TOP-tier юрфирмы** в сфере ПД, сами консультируем и несем ответственность

всегда приоритетно предлагаем установить систему на сервера клиента

даем клиенту **полный контроль** над защитой данных, авторизацией, установкой средств защиты и т.д.

если ставим систему в облаке — работаем с Яндекс Облаком

аудируем и сопровождаем Яндекс Облако по ПД как юристы, уверены и готовы платить за безопасный сервис

проходили многократные пентесты и проверки топ-провайдерами услуг по ИБ

регулярно проверяемся сами и никогда не отказываем клиентам в **повторной проверке** своими силами

Нужно попробовать!



 smartkedo.pro

Заходите на наш сайт и оставляйте [заявку на демо](#)



 sales@comply.ru

Попробовать [SmartКЭДО](#),
по всем вопросам касательно системы

 product@comply.ru

Если хотите поговорить про КЭДО,
задать вопрос, спросить совет

 t.me/smartkedo

Подписывайтесь на наш Telegram

- Полезный контент
- Анонсы вебинаров
- Лайфхаки и советы



До конца 2024 предлагаем модуль График отпусков [бесплатно](#) при приобретении нашей системы КЭДО



[Скидка 20%](#) на проект по внедрению системы КЭДО для всех зрителей вебинара по промокоду [ПД](#) до конца 2024