

Как работать с персональными данными в 2025 году: полное руководство

Если ваша организация работает с персональными данными (ПДн) — например, собирает телефоны клиентов, хранит паспортные данные сотрудников или использует сервисы аналитики на сайте, — она считается оператором и обязана соблюдать ФЗ от 27.07.2006 №152-ФЗ. Нарушения грозят штрафами до 20 млн рублей, потерей доверия клиентов и контрагентов.

Разбираемся, как безопасно работать с персональными данными компании, ИП или самозанятому, какие документы подготовить и как избежать штрафов.

Что такое персональные данные

Согласно ст. 3 ФЗ №152-ФЗ, персональные данные — это любая информация, прямо или косвенно относящаяся к конкретному человеку (субъекту ПДн). Это не только очевидные сведения вроде ФИО, даты рождения или серии и номера паспорта, но и:

- контакты (email, телефон);
- биометрические данные: отпечатки пальцев, фото и пр. (письмо Роскомнадзора от 10.02.2020 № 08АП-6782);
- IP-адрес, cookie-файлы (если по ним можно идентифицировать человека);
- геолокация, история покупок, даже должность и зарплата.

Пример: интернет-магазин, который запрашивает адрес доставки и номер телефона при регистрации. Эта информация относится к ПДн, а организация считается оператором. То же касается HR-отдела, который хранит резюме соискателей, или сервиса онлайн-записей, фиксирующего ПДн клиентов.

Закон требует от компаний, работающих с персональными данными, не только собирать их легально, но и обеспечивать безопасность, получать согласие на обработку и правильно оформлять внутреннюю документацию. Ошибки могут привести к серьезным штрафам.

Когда нужно согласие на обработку

Согласие на обработку оформляется в письменном или электронном виде добровольно самим субъектом ПДн. Оно не требуется лишь в исключительных случаях, перечисленных в п. 2–11 ч. 1 ст. 6 ФЗ № 152-ФЗ.

Пример: если ваша компания обрабатывает ПДн клиентов для доставки товаров, согласие нужно. Если же данные используются для исполнения судебного акта или обязательств перед сотрудником по трудовому договору — нет.

Что должно быть в согласии на обработку ПДн (ч. 4 ст. 9 ФЗ № 152-ФЗ):

1. Кто дает согласие: ФИО и реквизиты документа, удостоверяющего личность.
2. Кто обрабатывает данные: название компании-оператора, ее контакты и реквизиты.
3. Цели обработки: получение рекламных рассылок, рассмотрение анкеты соискателя на вакантную должность, и пр.
4. Какие действия с данными разрешены: сбор, запись, хранение, уточнение, передача, удаление и другие способы обработки (ст. 3 ФЗ №152-ФЗ).
5. Какие именно данные обрабатываются: например, ФИО, телефон, e-mail, паспортные данные или геолокация.
6. Сведения о третьем лице, которому поручена обработка (если оператор поручил работу с ПДн): наименование организации или ФИО и адрес такого лица.
7. Срок действия согласия: он может быть привязан к конкретной дате, к моменту достижения цели обработки или к отзыву согласия самим субъектом.
8. Подпись субъекта ПДн.

Важно! Если субъект ПДн недееспособен, согласие дает его законный представитель — опекун или попечитель. Если

оператор планирует распространять ПДн, нужно отдельное согласие субъекта на это (ст. 10.1 ФЗ № 152-ФЗ): например, для размещения фотографии и ФИО на доске почета или сайте организации.

Какие документы должны быть для работы с ПДн

Помимо шаблонов согласий, оператору нужно оформить еще ряд документов, назначить ответственного, и только после этого подать уведомление в Роскомнадзор для регистрации в реестре. Это обязательное требование, за исключением случаев, предусмотренных п. 7–9 ч. 2 ст. 22 ФЗ № 152-ФЗ, когда регистрация не требуется.

Для законной работы с персональными данными в организации должен быть следующий пакет документов:

- Копии уведомлений для Роскомнадзора в зависимости от ситуации:
 - о начале обработки ПДн;
 - об изменении сведений в ранее поданном уведомлении;
 - о прекращении обработки;
 - о трансграничной передаче данных.
- Акты.
- Журналы.
- Локальные акты: инструкции, положения, правила.
- Политика обработки ПДн.
- Приказы.
- Согласия.
- Иные документы.

Важно: этот перечень не исчерпывающий — в зависимости от специфики деятельности компании могут потребоваться дополнительные документы. Чтобы избежать ошибок и штрафов, лучше доверить подготовку документов юристам.

Требования к основным документам

Самый главный документ, на основании которого оператор оформляет другие документы — Политика обработки ПДн. Рекомендации по ее составлению даны Роскомнадзором.

Политика должна включать:

1. Общие положения:
 - определения ключевых терминов (обработка, оператор, субъект ПДн, конфиденциальность);
 - права и обязанности оператора и субъектов данных.
2. Цели обработки:
 - четкий перечень целей сбора данных (например, исполнение договора, кадровый учет, маркетинг);
 - запрет на обработку, не связанную с этими целями.
3. Правовые основания:
 - федеральные законы и Кодексы (например, ТК, НК);
 - согласие субъекта (если требуется);
 - договор.
4. Категории данных и субъектов:
 - какие данные обрабатываются (ФИО, контакты, паспортные данные и т. д.).
 - категории субъектов: сотрудники, клиенты, контрагенты.
5. Порядок обработки:
 - способы обработки (автоматизированные/ручные);
 - сроки хранения;
 - условия передачи третьим лицам (только при наличии договора).
6. Защита и хранение:
 - меры защиты;
 - требование хранить ПДн только в российских базах.
7. Работа с запросами субъектов:
 - порядок исправления, удаления данных;
 - регламент ответов на обращения (сроки, формы запросов).

Важно! Политика должна быть конкретной и соответствовать реальным бизнес-процессам. Нельзя просто так скачать образец из интернета и использовать его. Кроме того, документ необходимо опубликовать на сайте (если он есть) и разместить на информационном стенде, иначе компанию оштрафуют.

Как подать уведомление о регистрации в Роскомнадзор и что нужно учесть

Подать уведомление можно двумя способами — онлайн на сайте РКН или в бумажном виде, обратившись в территориальное отделение ведомства. Для подачи онлайн

нужен подтвержденный аккаунт на Госуслугах или установленный и настроенный плагин КриптоПро ЭЦП Browser plug-in.

Что важно учитывать:

1. Регион регистрации, наименование, адрес и другие сведения об операторе должны совпадать с данными ЕГРЮЛ или ЕГРИП.

2. Если у компании есть филиалы, они обязательно указываются.

3. Цели обработки ПДн — только те, для которых данные действительно требуются. Не нужно дописывать лишнее «на будущее».

4. Дата начала обработки данных — это дата начала фактической работы с ПДн (обычно дата регистрации компании или ИП).

5. Если уведомление отправляет не руководитель организации, понадобится доверенность.

Важно! Цели обработки должны совпадать с категориями субъектов ПДн и категориями обрабатываемых данных. Для этого, помимо ФЗ № 152-ФЗ, нужно знать ряд других законов. Например, вы не можете указать в качестве цели ведение кадрового и бухгалтерского учета, если собираете данные только для маркетинговых рассылок и продажи товаров.

Как правильно хранить персональные данные

Нельзя хранить персональные данные клиентов или сотрудников просто так — закон требует соблюдения четких правил. Согласно ч. 7 ст. 5 ФЗ № 152-ФЗ, данные должны храниться только в течение срока, необходимого для целей их обработки. Например, если вы собираете телефоны для доставки, то после выполнения заказа эти данные уже не нужны — их надо удалить или обезличить.

Исключение — случаи, когда срок хранения прямо указан в законе или договоре с клиентом. Но все равно по достижении срока или отдельных условий ПДн нужно уничтожить.

Правила уничтожения персональных данных

ПДн уничтожаются по окончании срока хранения или по запросу субъекта. Для этого необходимо создать комиссию и выбрать способ уничтожения в зависимости от вида носителя:

1. Электронные документы:

- Физическое разрушение носителей (если данные больше не нужны):
 - диски, флешки, жесткие диски дробятся или перемагничиваются (ГОСТ Р 50739-95);
 - SSD-накопители требуют специального оборудования — простое удаление файлов недостаточно.
- Удаление из программы:
 - использование сертифицированных программ для затирания;
 - шифрование с последующим удалением ключей (если данные были зашифрованы, их нельзя восстановить).

2. Бумажные документы:

- шредирование (измельчение) — минимальный стандарт: частицы не более 5 мм (для конфиденциальных данных);
- сжигание — подходит для особо важных документов, но требует соблюдения экологических норм.

По результатам уничтожения составляется акт. Если ПДн хранились в электронном виде, понадобится выгрузка регистрации событий в ИС.

Ответственность и штрафы

Оператор несет ответственность за любые нарушения при обработке. **Суммы штрафов** зависят от типа правонарушения и статуса нарушителя (физлицо, должностное лицо, ИП, юрлицо).

Основные нарушения и штрафы предусмотрены ст. 13.11 КоАП:

1. Обработка данных без законных оснований или не в соответствии с целями сбора:

- граждане: от 10 000 до 15 000 рублей;
- должностные лица: от 50 000 до 100 000 рублей;
- юрлица: от 150 000 до 300 000 рублей;

2. Обработка без согласия субъекта, когда оно обязательно:

- граждане: от 10 000 до 15 000 рублей;
- должностные лица: от 100 000 до 300 000 рублей;
- юрлица: от 300 000 до 700 000 рублей.

3. Неопубликование Политики обработки ПДн:

- граждане: от 1 500 до 3 000 рублей;
- должностные лица: от 6 000 до 12 000 рублей;
- ИП: от 10 000 до 20 000 рублей;
- юрлица: от 30 000 до 60 000 рублей.

Также есть штрафы за непредоставление субъекту информации о его ПДн — до 80 000 рублей. Если оператор по запросу субъекта не удалит его данные, могут оштрафовать на сумму до 90 000 рублей. За отсутствие регистрации в реестре организаций, работающих с персональными данными — до 300 000 рублей. При утечке данных штрафы могут достигать 20 млн, за повторное нарушение — 500 млн рублей или 3% годового оборота организации-оператора.

Заключение

Работа с персональными данными в 2025 году требует строгого соблюдения ФЗ № 152-ФЗ. Ошибки чреваты штрафами в сотни миллионов рублей и репутационными потерями. Чтобы минимизировать риски, правильно подготовьте шаблоны согласий и других документов для обработки ПДн, подайте уведомление в Роскомнадзор, следите за сроками хранения и своевременно уничтожайте данные.