

Что входит в состав персональных данных

С 30 мая 2025 года в силу вступают существенные изменения в сфере защиты персональных данных — увеличиваются штрафы за нарушения, связанные с их обработкой, а также вводятся новые меры ответственности. Это результат обновлений, внесённых Федеральным законом от 30.11.2024 № 420-ФЗ в Кодекс об административных правонарушениях (КоАП РФ). Чтобы не попасть под санкции, работодателям важно точно понимать, какие данные считаются персональными, как их законно собирать, обрабатывать и защищать.

Что считается персональными данными

Согласно п. 1 ст. 3 Федерального закона № 152-ФЗ, персональными считаются любые сведения, позволяющие прямо или косвенно идентифицировать конкретного человека, который называется субъектом персональных данных. Самы по себе ФИО не являются персональными данными, но в сочетании с другими сведениями (например, дата рождения, адрес, телефон, СНИЛС) они уже подпадают под защиту закона.

Пример:

- «Алина Сергиенко» — не персональные данные
- «Алина Сергиенко, СНИЛС 112-233-445 66, e-mail: alser@mail.ru» — персональные данные

Основные категории персональных данных

Закон выделяет три типа персональных данных:

- Обычные (основные) — ФИО, паспортные данные, контактная информация, место жительства. На бланке уведомления они названы просто “Персональными данными”:

<p>Категории персональных данных, осуществляющих обработку</p>	Персональные данные	
	<input type="checkbox"/> фамилия, имя, отчество	<input type="checkbox"/> год рождения
	<input type="checkbox"/> месяц рождения	<input type="checkbox"/> дата рождения
	<input type="checkbox"/> место рождения	<input type="checkbox"/> семейное положение
	<input type="checkbox"/> социальное положение	<input type="checkbox"/> имущественное положение
	<input type="checkbox"/> доходы	<input type="checkbox"/> пол
	<input type="checkbox"/> адрес электронной почты	<input type="checkbox"/> адрес места жительства
	<input type="checkbox"/> адрес регистрации	<input type="checkbox"/> номер телефона
	<input type="checkbox"/> СНИЛС	<input type="checkbox"/> ИНН
	<input type="checkbox"/> гражданство	<input type="checkbox"/> данные документа, удостоверяющего личность
	<input type="checkbox"/> данные водительского удостоверения	<input type="checkbox"/> данные документа, удостоверяющего личность за пределами Российской Федерации
	<input type="checkbox"/> данные документа, содержащиеся в свидетельстве о рождении	<input type="checkbox"/> реквизиты банковской карты
	<input type="checkbox"/> номер расчетного счета	<input type="checkbox"/> номер лицевого счета
	<input type="checkbox"/> профессия	<input type="checkbox"/> должность
	<input type="checkbox"/> сведения о трудовой деятельности (в том числе стаж работы, данные о трудовой занятости на текущее время с указанием наименования и расчетного счета организации)	<input type="checkbox"/> отношение к воинской обязанности, сведения о воинском учете
	<input type="checkbox"/> иные персональные данные	<input type="checkbox"/> сведения, собираемые посредством метрических программ
	<input type="checkbox"/> сведения об образовании	<input type="checkbox"/> фото-видео изображение лица
	<input type="checkbox"/> данные голоса человека	

2. Специальные — сведения о расе, национальности, политических или религиозных убеждениях, состоянии здоровья, интимной жизни. Их можно обрабатывать только при наличии письменного согласия. Вот как специальные персданные выглядят на бланке уведомления:

Специальные категории персональных данных

- сведения о состоянии здоровья национальная принадлежность
- политические взгляды религиозные или философские убеждения
- сведения о судимости

3. Биометрические — данные, позволяющие установить личность (например, фото, отпечатки пальцев, скан радужной оболочки глаза). Также требуют отдельного согласия.

Когда бизнесу нужно собирать персональные данные

Сбор ПД неизбежен в ряде типичных ситуаций:

1. При найме, увольнении, ведении кадрового учёта.
2. При сдаче отчётности (по НДФЛ, страховым взносам и т.п.).
3. Для проведения маркетинга, изучения целевых аудиторий.
4. При продаже товаров или услуг через интернет.
5. При обеспечении безопасности (например, установке видеонаблюдения).

Обязанности оператора персональных данных

Оператором ПД считается любое лицо или учреждение, которая обрабатывает персональные данные — будь то компания, ИП, физлицо или госорган.

Что обязан сделать оператор:

1. Подготовить локальные документы:
 - политику в отношении обработки ПД
 - приказы о назначении ответственных лиц
 - обязательства о конфиденциальности
2. Подать уведомление в Роскомнадзор (если применяется автоматизированная обработка). Формы и способы подачи — через сайт Роскомнадзора, почту или портал Госуслуг. При изменении данных, отражённых в уведомлении, нужно направить уведомление о корректировке.
3. Обеспечить законность сбора данных — с получением согласия субъекта.

Отметим, что оператор персданных вправе обойтись без регистрации в реестре, если не автоматизирует их обработку, то есть, не пользуется компьютером, а записывает всё на бумаге и хранит в аналоговой картотеке (часть 2 статьи 22 Закона № 152-ФЗ).

Операторы довольно часто ошибаются при заполнении уведомлений. Чаще всего адрес оператора пишут не полностью и забывают часть категорий субъектов персданных. Подробнее о популярных нарушениях можно прочесть в статье «Типовые ошибки в уведомлении об обработке персональных данных».

Согласие на обработку ПД: когда и как его оформлять

Согласие — основной правовой инструмент, подтверждающий, что человек разрешает обработку своих данных. Оно по закону (часть 1 статьи 6 Закона № 152-ФЗ) необходимо практически всегда, кроме случаев, прямо предусмотренных законом (например, для исполнения трудового договора). Строго определённого бланка для этого документа нет.

Формы согласия:

1. В письменном виде — для обычных, специальных и биометрических данных.

2. В электронной форме — только для обычных данных при дистанционном взаимодействии (например, галочка на сайте).

Примеры ситуаций, когда требуется согласие:

- приём сотрудника и хранение его документов
- передача данных страховой или иной третьей стороне
- видеонаблюдение на рабочем месте
- регистрация на сайте, заказ товара в интернет-магазине

Внимание! Обработка персданных означает производить с ними какие-либо действия, то есть, собирать персданные, записывать, систематизировать, хранить, копить, редактировать, обновлять, извлекать, использовать, удалять и так далее. Помимо этого, сюда относятся передача информации, т. е., её публикация, предоставление и доступ (пункт 3 статьи 3 Закона № 152-ФЗ).

При сетевом взаимодействии, например, при онлайн-продаже товаров, согласие на обработку персональных данных часто получают путём установки галочки в соответствующем поле под размещённым на сайте документом — таким, как политика конфиденциальности, пользовательское соглашение и т.п. Однако, стоит учитывать, что такой способ подтверждения согласия не применим, если речь идёт о сборе специальных или биометрических персональных данных — в этих случаях необходимо письменное согласие.

Приведём типичные ситуации, в которых требуется получение согласия на обработку персональных данных:

- оформление сотрудника на работу и хранение копий его личных документов
- передача трудовой книжки работника сторонним организациям, например, в страховую компанию
- установка видеонаблюдения или аудиоконтроля на рабочих местах сотрудников
- продажа продукции через онлайн-магазины
- сбор пользовательской информации при регистрации на онлайн-сервисах и создании личных кабинетов

Почему важно защищать персональные данные

Персональные данные нередко становятся целью злоумышленников. С их помощью могут:

1. Заключать фиктивные сделки.
2. Получать доступ к аккаунтам.
3. Использовать информацию для социальной инженерии или выманивания денег.

Как защитить данные: рекомендации для работодателей

1. Ограничьте доступ: определите, кто из работников может работать с персданными, и закройте доступ к ним остальному персоналу.
2. Разделите данные: используйте обезличивание (например, в одной базе — ФИО, в другой — телефоны, связанные с кодами).
3. Проводите аудит: регулярно проверяйте, как защищены ваши данные, и устраняйте риски.

Штрафы и ответственность с 30 мая 2025 года

С 30 мая вступают в силу ужесточённые меры ответственности (Федеральный закон от 30.11.24 № 420-ФЗ). Нарушения в сфере обработки ПД теперь караются крупными штрафами,

особенно в случае массовых утечек (новые **части 13 и 14 статьи 13.11** КоАП):

- от 10 000 до 100 000 человек — штрафы в десятки миллионов рублей
 - более 100 000 человек — штрафы ещё выше, с возможностью блокировки ресурсов
- Вводятся санкции не только за сам факт утечки, но и за ненадлежащее хранение, отсутствие согласия, и т.д. В таблице приведены старые и новые формы штрафов для разных категорий нарушителей:

Категория плательщиков	До 30 мая 2025 года	С 30 мая 2025 года
Обработка ПД в случаях, не предусмотренных законом (ч. 1 ст. 13.11 КоАП)		
Физлица	2-6 тыс. руб.	10-15 тыс. руб.
Должностные лица и ИП	10-20 тыс. руб.	50-100 тыс. руб.
Организации	60-100 тыс. руб.	150-300 тыс. руб.
Обработка специальных и (или) биометрических ПД без письменного согласия субъекта (ч. 2 ст. 13.11 КоАП)		
Физлица	10-15 тыс. руб.	
Должностные лица и ИП	100-300 тыс. руб.	
Организации	300-700 тыс. руб.	
Неуведомление Роскомнадзора об обработке персданных (ст. 19.7, новая ч. 10 ст. 13.11 КоАП)		
Физлица	100-300 руб.	5-10 тыс. руб.
Должностные лица и ИП	300-500 руб.	30-50 тыс. руб.
Организации	3-5 тыс. руб.	100-300 тыс. руб.
Неуведомление Роскомнадзора об утечке персданных (новая ч. 11 ст. 13.11 КоАП)		
Физлица	штраф не предусмотрен	50-100 тыс. руб.
Должностные лица и ИП		400-800 тыс. руб.
Организации		1-3 млн руб.
Действия (бездействие), повлекшие утечку персданных 1 тыс. до 10 тыс. человек (новая ч. 12 ст. 13.11 КоАП)		
Физлица	штраф не предусмотрен	100-200 тыс. руб.
Должностные лица и ИП		200-400 тыс. руб.
Организации		3-5 млн руб.

Вывод

Соблюдение требований закона о персональных данных — не просто формальность, а необходимое условие безопасной и законной деятельности. Новые правила и повышенные

штрафы обязывают работодателей более внимательно относиться к каждой стадии работы с персональной информацией: от сбора до уничтожения. Не дожидайтесь проверок и санкций — проверьте, насколько ваша фирма соответствует требованиям уже сегодня.

Если вам нужна помощь с оформлением политики обработки ПД, подготовкой уведомлений или составлением согласий — обратитесь к юристу или специалисту по защите информации.

Читайте также План проверок Роструда на 2025 год