



Как избежать штрафов :
Актуальные вопросы трудового законодательства:
Хранение персональных данных:
как организовать и какие особенности учесть
Готовые кадровые решения

г. Иваново, 12 мая 2022 г.



Дистанционные и выездные услуги:



**КОНСУЛЬТАЦИИ, КАДРОВЫЕ СЛУЖБЫ «С НУЛЯ»,
АУДИТ СОБЛЮДЕНИЯ ТРУДОВОГО
ЗАКОНОДАТЕЛЬСТВА, ПОДГОТОВКА К ПРОВЕРКАМ
ГИТ, ОБУЧЕНИЕ, РЕГЛАМЕНТАЦИЯ РАБОТЫ
КАДРОВЫХ СЛУЖБ, РАЗРАБОТКА И РЕАЛИЗАЦИЯ
СТРАТЕГИЙ РАБОТЫ С ПЕРСОНАЛОМ,
ОПТИМИЗАЦИЯ ЧИСЛЕННОСТИ, СХЕМЫ
МОТИВАЦИИ**

Записаться на установочную (бесплатную)
консультацию можно:

- на сайте <https://hr37.ru>
- В Telegram-канале https://t.me/tatyana_kosterina_hr37
- в Telegram, WhatsApp, Viber , телефон - +7(910) 994-90-37
- по электронной почте - t.a.costerina@gmail.com

ВАШЕ СПОКОЙСТВИЕ – МОЯ РАБОТА!



Нормативная база

- Конституция Российской Федерации (ст. 23, 24);
- Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (Глава 14 – «Защита персональных данных работника»);
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных»;
- Федеральный закон № 149 от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;



Нормативная база

- Постановление Правительства РФ от 21.03.2012 N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;
- Постановление Правительства РФ от 19.08.2015 № 857 «Об автоматизированной информационной системе «Реестр нарушителей прав субъектов персональных данных»;
- Приказ Роскомнадзора от 05.09.2013 N 996 "Об утверждении требований и методов по обезличиванию персональных данных».
- Указ Президента России от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»



Документы для заключения трудового договора

Документ	Для чего требуется
Паспорт	Документ, удостоверяющий личность
Трудовая книжка/Сведения о трудовой деятельности	Стаж, опыт работы
СНИЛС	<u>С 2019 г. форма АДИ-РЕГ</u>
Военный билет	Если работник военнообязанный или призывник
Диплом, другие документы об образовании	Подтверждение квалификации, наличии специальной подготовки если соискатель поступает на должность, требующую особых знаний
Справка о судимости / уголовном преследовании либо о его прекращении	Для работ, к которым не допускаются судимые или подвергшиеся уголовному преследованию



Основные понятия (ст. 5 п.5 закона 152-ФЗ)

ОПЕРАТОР - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

Неавтоматизированная
обработка персональных
данных

Автоматизированная обработка
персональных данных - обработка
персональных данных с помощью
средств вычислительной техники

**ПЕРСОНАЛЬНЫЕ
ДАННЫЕ РАБОТНИКОВ**

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ -
любое действие (операция) или
совокупность действий (операций),
совершаемых с использованием средств
автоматизации или без использования
таких средств с персональными данными,
включая сбор, запись, систематизацию,
накопление, хранение, уточнение
(обновление, изменение), извлечение,
использование, передачу
(распространение, предоставление,
доступ), обезличивание, блокирование,
удаление, уничтожение персональных
данных



Основные понятия (ст.3. закона 152-ФЗ)

Персональные данные (ПД) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Персональные данные работника - это информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника (ст.85 ТК РФ). В соответствии со ст.3 Федерального закона №152-ФЗ "О защите персональных данных", к персональным данным относятся:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- адрес;
- семейное, социальное, имущественное положение;
- образование;
- профессия;
- доходы;
- другая информация.

Специальные персональные данные – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни

Биометрические персональные данные – сведения, характеризующие физиологические особенности человека, на основе которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных

Иные ПД – не могут быть включены в первые три категории.



Основные понятия

- **Обработка ПД** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПД, включая ... **передачу** (распространение, предоставление, доступ)...;
- **Предоставление** ПД — это их раскрытие (передача) конкретному лицу или кругу лиц;
- **Распространение** ПД — это их передача неопределенному кругу лиц.

Отменено понятие *общедоступных персональных данных*.



Объем ПД работника, которые подлежат обработке и хранению (ст. 5 п.5 закона 152-ФЗ)

Объем должен соответствовать с целями обработки, которые вами заявлено в Политике или других ЛНА:

Основной регламентирующий документ — Трудовой кодекс:

Ст. 86 содержит перечень норм, которыми стоит руководствоваться при расчете объема и содержания ПД.

Ст. 65 ТК дает полный список документов с персональными сведениями, которые наниматель может требовать у сотрудника для заключения трудового договора.

Статья 65 ТК РФ не называет какие персональные данные может хранить и обрабатывать работодатель или сотрудник кадровой службы на протяжении трудовой деятельности работника. В статье перечислены документы, которые предъявляются при заключении трудового договора.



Согласие на обработку персональных данных (п.1 ст. 6 закона 152-ФЗ)

Обработка ПД возможна только с согласия работника (п.1.ст 6 закона 152-ФЗ)
Согласие на обработку персональных данных – это разрешение гражданина РФ, которое он дает заинтересованной стороне на получение, сбор, хранение и использование персональных данных о себе.

Согласие гарантирует человеку то, что информация о нем будет применяться для строго определенных целей и будет защищена от неправомерных действий. Назначение согласия – защитить права *гражданина (субъекта ПД)*.

В спорных ситуациях Работодатель обязан доказать, что получил согласие (ч.3 ст.9 закона 152-ФЗ), поэтому согласие лучше получить в письменном виде.

Справочно: Документ «Согласие на обработку персональных данных» введён в оборот в 2007 г. с принятием закона № 152-ФЗ «О персональных данных».



Согласие на обработку персональных данных

1. Оператор имеет право обрабатывать (т.е. собирать, предавать, записывать, хранить) только те ПД, на которые получено письменное согласие субъекта ПД. (п.1.ст 6 закона 152-ФЗ)
2. В согласии прописываются правила обработки, хранения и использования организацией персональных данных (ПД) работников компании. Полный перечень сведений в согласии – (ч.4.ст. 9 закона 152-ФЗ)
3. В случае, если сотрудник не дал согласия на распространение ПД, но при этом дал согласие на обработку, то работодатель не в праве распространять ПД и передавать ее третьим лицам (п. 4 ст. 10.1 Закона № 152-ФЗ).
4. Работник в любое время может отозвать согласие на обработку ПД (ч.2 ст. 9 закона 152-ФЗ)



Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (Приказ Роскомнадзора от 24.02.2021 № 18)

Согласие должно содержать следующую информацию:

- 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-организации** - *наименование, адрес, указанный в ЕГРЮЛ, ИНН, ОГРН (если он известен субъекту персональных данных);*
- 4) **сведения об информационных ресурсах оператора** (*адрес, состоящий из наименования протокола (http или https), сервера (www), домена, имени каталога на сервере и имя файла веб-страницы*), посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных;
- 5) **цель (цели) обработки персональных данных;**



Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения (Приказ Роскомнадзора от 24.02.2021 № 18)

б) категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных:

-персональные данные (фамилия, имя, отчество (при наличии), год, месяц, дата рождения, место рождения, адрес, семейное положение, образование, профессия, социальное положение, доходы, другая информация, относящаяся к субъекту персональных данных);

-специальные категории персональных данных (расовая, национальная принадлежности, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимной жизни, сведения о судимости);

-биометрические персональные данные.

7) категории и перечень ПД, для обработки которых субъект ПД устанавливает условия и запреты, а также перечень устанавливаемых условий и запретов (заполняется по желанию субъекта ПД);

8) условия, при которых полученные ПД могут передаваться оператором, осуществляющим обработку ПД, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных)

9) срок действия согласия.



Когда нет необходимости в оформлении отдельного согласия (пункт 5 статьи 6 ФЗ-№152)

Передача и обработка личных сведений физического лица должно производиться исключительно с его согласия.

Однако, согласие работников на обработку личных сведений можно не брать:

- В случае, если организация занимается обработкой этих данных и это прописано в трудовом договоре
- Работодателям необходимы данные сотрудников для начисления заработной платы, ведения кадровой документации и других видов отчетности.
- При передаче сведений в ФНС, ПФР, ФСС, военный комиссариат, судебным приставам, в прокуратуру и иные государственные ведомства.
- В финансовые учреждения для оформления зарплатных карт, если в нормативном акте об оплате труда прописано получение зарплаты на банковскую карту и есть факт согласия сотрудника.



На какой срок оформить согласие на обработку ПД?

Оформить согласие на обработку персональных данных без срока обработки нельзя.

Однако определить его можно не только календарной датой или периодом времени, но также событием.

Например, в бланке можно прописать, что согласие действует, пока его не отзовет субъект. Главное, чтобы такой срок был оправданным с учетом цели обработки персональных данных. В тексте согласия распишите, как субъект сможет согласие отозвать. Для удобства лучше сделать шаблон письменного отзыва и выложить его на сайте, откуда его можно будет свободно скачать. Так вы продемонстрируете, что не только соблюдаете правила работы с персональными данными, но также обеспечиваете субъектам возможность реализации их прав в этой области.



Хранение ПД соискателей (Абз.11п.5 Разъяснения Роскомнадзора от 14 декабря 2012 года «ВОПРОСЫ, КАСАЮЩИЕСЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, СОИСКАТЕЛЕЙ НА ЗАМЕЩЕНИЕ ВАКАНТНЫХ ДОЛЖНОСТЕЙ, А ТАКЖЕ ЛИЦ, НАХОДЯЩИХСЯ В КАДРОВОМ РЕЗЕРВЕ»)

Согласие на обработку ПД необходимо получать не только от работников, но и от соискателей.

Вывод:

За хранение резюме соискателей можно получить штраф от Роскомнадзора, потому что там тоже содержатся персональные данные.

Резюме разрешается использовать в течение срока, пока сотрудник кадровой службы рассматривает потенциальных кандидатов.

Не храните резюме ни в распечатанном виде, ни в электронном, например, присланный на e-mail, если вакансия уже закрыта. Если в компании формируется кадровый резерв, у каждого кандидата необходимо брать у каждого кандидата возьмите согласие на хранение сведений о нем и укажите цель хранения.



Распространение ПД

Обработка ПД может предполагать передачу ПД.

1. Передача ПД может осуществляться путем их распространения, предоставления или открытием доступа.
2. Распространение ПД — это один из видов передачи данных, при котором ПД раскрываются неопределенному кругу лиц.
3. Термины «распространение», «предоставление» не являются синонимами — это разные виды передачи ПД.

Эти выводы важны, т.к. позволяют четко разделить, когда происходит **распространение** (данные видит неограниченный круг лиц), а когда **предоставление** (данные получают строго определенные лица).

Распространяет ли работодатель ПД своих работников?

Другими словами: **раскрывает ли работодатель ПД работников неопределенному кругу лиц?**

Ответ: «Нет, не раскрывает» является ошибочным.

Что такое раскрытие «неопределенному кругу лиц»?

Это значит, что любой человек может свободно увидеть ПД, специально не скрытые: Ф. И. О., должность, телефон, адрес, размер зарплаты, дату рождения, адрес личной электронной почты, личный телефонный номер, фото- и видеоизображение и пр.



Распространение ПД

- Особенности обработки ПД, разрешенных субъектом для распространения, определяет **новая статья 10.1** Закона № 152-ФЗ.
- **Согласие на обработку ПД, разрешенных субъектом для распространения, оформляют отдельно от иных его согласий на обработку его ПД**
- **Субъект в Согласии на обработку ПД, разрешенных для распространения, вправе установить запреты на:**
 - **передачу (кроме предоставления доступа) этих ПД оператором неограниченному кругу лиц;**
 - **обработку или условия обработки (кроме получения доступа) этих ПД неограниченным кругом лиц.**
- **Оператор не может отказать в установлении субъектом запретов и условий.**



Согласие на распространение ПД(ст. 10.1. закона №152-ФЗ

1. Согласие на обработку ПД, которые разрешены субъектом для распространения оформляется отдельно.
2. Оператор должен предоставить возможность субъекту ПД определить список тех ПД, которые он разрешает распространять по каждой категории ПД.
3. Если субъект раскроет свои личные данные, но не предоставит согласие, обязанность доказать правомерность их распространения лежит на всех лицах, которые распространили эти сведения.

Пример: Если в одном источнике опубликована информация, содержащая ПД, то доказать правомерность ее использования должны будут все издания, перепечатавшие эти сведения. Таким образом, все источники информации обязаны спрашивать у героев своих публикаций, какие данные о них можно публиковать и передавать третьим лицам.



Согласие на распространение ПД(ст. 10.1. закона №152-ФЗ

4. Примерно то же, что и предыдущий пункт (№3), но источник ПД — нарушения, преступления или обстоятельства непреодолимой силы.
5. В согласии должно быть четко сформулировано, на что конкретно согласен субъект.
6. Если субъект ПД не согласен с распространением или не указал специальные условия обработки для некоторых категорий ПД и их перечня — такие сведения можно только обрабатывать без распространения (передачи, предоставления и иных действий) неограниченному кругу лиц.
7. Способы получения согласия на распространение ПД от субъекта ПД::
 - непосредственно на бумаге с личной подписью;
 - через информационную систему Роскомнадзора.

Совет:

В согласии должно быть абсолютно понятно, что можно делать с ПД, а что нельзя. Если что-то вызывает сомнения — лучше ничего не публиковать.



Содержание согласия на распространение ПД (Приказ Роскомнадзора Роскомнадзора от 24.02.2021 N 18 Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения)

Согласие должно быть составлено письменно и содержать:

данные физического лица, дающего согласие, то есть фамилия, имя, отчество, личный телефон, адрес и электронную почту;

- данные организации, которая получает информацию о гражданине – ее наименование, юридический адрес, ЕГРЮЛ, ОГРН, ИНН;
- цель для обработки сведений о физическом лице, к примеру, публикация данных на личном портале осуществляется для роста продаж и увеличения доверия клиентов;
- группы и список данных, то есть человек обязан перечислить, какую именно информацию он разрешает или не разрешает обрабатывать;
- период действия данного согласия, то есть временной интервал, когда действует настоящее согласие, дата начала и окончания;
- название ресурса, где человек разрешает размещать личные данные с указанием конкретного раздела в случае, если сведения будут подвержены публикации.

С 1 июля 2021 года согласие на обработку личных данных физические лица могут направить посредством информационной системы Роскомнадзора.

руководителю _____

адрес местонахождения: _____

ОГРН: _____, ИНН: _____

ОКВЭД: _____, ОКПО: _____, ОКОГУ: _____,

ОКОПФ: _____, ОКФС: _____

от _____,

паспорт серии ____ № ____ выдан «__» ____ года

зарегистрированного(ой) по адресу: _____

адрес электронной почты: _____

номер телефона: _____

**Согласие на обработку персональных данных,
разрешенных субъектом персональных данных для распространения**

Настоящим я, _____,
руководствуясь статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ
«О персональных данных», заявляю о согласии на распространение

Наименование организации

моих персональных данных с целью размещения информации обо мне
на официальном сайте и корпоративном портале _____

_____ в следующем порядке:

Наименование организации

Категория персональных данных	Перечень персональных данных	Разрешаю к распространению (да/нет)	Разрешаю к распространению неограниченному кругу лиц (да/нет)	Условия и запреты	Дополнительные условия
общие персональные данные	фамилия	<i>да</i>	<i>да</i>		
	имя	<i>да</i>	<i>да</i>		
	отчество	<i>да</i>	<i>да</i>		
	год рождения	<i>нет</i>			
	месяц рождения	<i>да</i>	<i>да</i>		
	дата рождения	<i>да</i>	<i>да</i>		
	место рождения	<i>да</i>	<i>нет</i>		<i>только сотрудникам ООО «Альфа»</i>
	адрес	<i>нет</i>			
	семейное положение	<i>да</i>	<i>нет</i>		<i>только сотрудникам ООО «Альфа»</i>
	образование	<i>да</i>	<i>нет</i>	<i>кроме ООО «Звезда»</i>	
	профессия	<i>да</i>	<i>нет</i>	<i>кроме ООО «Звезда»</i>	
	...				
специальные категории персональных данных	состояние здоровья	<i>да</i>	<i>нет</i>		<i>только сотрудникам отдела кадров</i>
	сведения о судимости	<i>да</i>	<i>нет</i>		<i>только сотрудникам отдела кадров</i>
	...				
биометрические персональные данные	цветное цифровое фотографическое изображение лица	<i>да</i>	<i>да</i>		

Сведения об информационных ресурсах Оператора, посредством которых будут осуществляться предоставление доступа неограниченному кругу лиц и иные действия с персональными данными субъекта персональных данных:

Информационный ресурс	Действия с персональными данными
https://alfa-alfa@.ru/	Предоставление сведений неограниченному кругу лиц
https://corp.alfa-alfa@.ru/	Предоставление сведений сотрудниками компании
...	

Настоящее согласие дано мной добровольно и действует с 01.03.2021 по 31.12.2021.

Оставляю за собой право потребовать прекратить распространять мои персональные данные. В случае получения требования Оператор обязан немедленно прекратить распространять мои персональные данные, а также сообщить перечень третьих лиц, которым персональные данные были переданы.

Подпись _____



Надо ли что-либо изменять в «старых» согласиях на обработку ПД работников? Проверяем старые согласия:

1 Если в тексте есть термин «распространение» ПД – его надо исключить, так как теперь он имеет новую трактовку

2 Если в тексте есть термин «передача» ПД – следует добавить «за исключением распространения неограниченному кругу лиц»

3 Если в тексте не упоминается ни распространение ПД, ни их передача – менять текст согласия не надо



Срок хранения персональных данных работника (ст. 5 п.7 №-152 ФЗ)

Срок хранения ПД определяют:

- федеральные законы;
- сам сотрудник (в договорах, согласии);
- достижение цели обработки.

Когда цель обработки ПД достигнута, личная информация обезличивается, уничтожается, если по отношению к ней не действуют другие нормы, к примеру, федеральные законодательные.

Срок действия разрешения субъекта на обработку его данных устанавливается на основании п. 4, 8 ст. 9 №152-ФЗ, а именно — до даты, указанной в самом документе.

Хранение согласий на обработку персональных данных нормирует Приказ Росархива от 20.12.2019 N 236 — 3 года после окончания этой даты или отзыва, если иное не предусматривается федеральными законами, договорами.

АКТ

15.08.2019

№ 37

Москва

Об уничтожении материальных носителей персональных данных

Настоящий акт составлен комиссией, созданной приказом ООО «Альянс» от 12.08.2019 № 37, в составе председателя — директора по персоналу Романова А.И., членов комиссии — начальника отдела кадров Оводова О.Л., юрисконсульта Лапина О.В.

Акт составлен о том, что комиссией были уничтожены материальные носители персональных данных работников ООО «Альянс» в следующем объеме:

№ п/п	Вид материального носителя персональных данных	Дата уничтожения	Процедура уничтожения материального носителя	Причина уничтожения материального носителя персональных данных
1	<i>Копия страниц паспорта (с личными данными, информацией о регистрации по месту жительства) Козлова О.Л.</i>	15.08.2019	<i>Измельчение в бумагорезательной машине</i>	<i>Достигнута цель обработки персональных данных</i>
2	<i>Копия свидетельства о рождении ребенка и страниц паспорта (информация с личными данными, сведения о семейном положении и детях) Малининой А.О.</i>	15.08.2019	<i>Измельчение в бумагорезательной машине</i>	<i>Достигнута цель обработки персональных данных</i>
3	<i>Служебная переписка об установлении персональных надбавок</i>	15.08.2019	<i>Измельчение в бумагорезательной машине</i>	<i>Истечение срока хранения</i>
...				

Содержание данного акта подтверждаем личными подписями:

...



Хранение ПД

Законами не определены правила хранения, обработки ПД.

Согласно ст. .87 ТК РФ работодатель вправе самостоятельно установить порядок обработки ПД, учитывая:

- предписания Приказа Росархива от 20.12.2019 N 236
- доступ к ПД уполномоченных на обработку и других лиц;
- способы работы с ПД, обрабатываемых на бумаге или в ЭДО;

Порядок обработки ПД устанавливается в локальном нормативном акте (ЛНА), который вводится в действие приказом.



Где можно взять информацию для определения положений ЛНА о ПД

- Ст.18.1 №152 ФЗ регламентирует, какие меры может предпринимать оператор и ответственный по охране ПД
- Условия, обеспечивающие надлежащую защиту персональных данных, подробно описаны в Постановлении Правительства от 21 марта 2012 г. N 211 и Постановлении Правительства от 15 сентября 2008 г. N 687
- К носителям биометрических данных предъявляются специальные требования. Особый порядок хранения таких сведений установлен Постановлением № 512 от 06 июля 2008 г.



Политика обработки персональных данных

Политика обработки персональных данных — это ЛНА, который определяет направления работы компании по обработке и защите персональных данных.

- Политика распространяется не только на сотрудников, но и на клиентов, контрагентов компании, иных третьих лиц.
- Как составить документ, разъяснил Роскомнадзор в Рекомендациях от 27.07.2017.

Важно не только разработать, но и опубликовать политику на сайте компании. Если его нет, то сделайте документ в бумажном виде доступным для всех заинтересованных лиц. Например, разместите в актовом зале, при входе в организацию и т. п.

Справочно: Если работодатель не разместил политику обработки персональных данных в открытом доступе, должностное лицо накажут на сумму от 3000 до 6000 руб., организацию — от 15 000 до 30 000 руб. (ч. 3 ст. 13.11 КоАП, п. 2 ст. 18.1 Федерального закона от 27.07.2006 № 152 ФЗ, далее — Закон № 152 ФЗ).



Политика обработки персональных данных позволяет

1. Назначить ответственного за организацию обработки персональных данных;
2. Разработать локальные акты по вопросам обработки персональных данных;
3. Определить круг допущенных к ПД;
4. Обеспечить применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
5. Организовать внутренний контроль соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, локальным актам оператора;
6. Провести оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона 152-ФЗ;
7. Ознакомить работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, и обучить указанных работников



Какие вопросы надо продумать для гарантии сохранности ПД в компании?

- Требования к месту, где хранятся персональные данные работников;
- Обеспечение сохранности конфиденциальной информации, исключение свободного проникновения или нахождения в помещениях посторонних лиц;
- Требования к ответственным за обработку ПД;
- Способы хранения персональных данных, содержащихся в бланках, — сейфы, запирающиеся шкафы, проч..



Хранение ПД на бумажных носителях

Бумажные носители с персональными данными:

- личные дела,
- трудовые книжки,
- договоры с работниками,
- бухгалтерские ведомости на выплату зарплаты или командировочных.
-

Рекомендации для хранения:

- держать бумаги нужно в сейфах или металлических негорючих шкафах, которые запираются на замок.
- По возможности оборудовать специальное помещение, например, отдельное помещение кассы со стальной дверью;
- ПД, обрабатываемые в разных целях, разумно хранить отдельно друг от друга,
- Документы с разным сроком хранения, лучше не смешивать;
- не хранить в личных делах : копии паспорта, СНИЛС и ИНН, свидетельства о браке или рождении ребенка, и все остальные, которые Роскомнадзор при проверке признает как содержащие избыточные персональные сведения.



Хранение ПД в электронном виде

Регламентируется в Постановлении Правительства РФ от 01.11.2012 № 1119.

- Информация может храниться на флешках или жестких дисках, сервере компании или удаленно в облачном хранилище;
- ПД хранятся столько времени, сколько нужно для обработки, а после следует их уничтожить или обезличить;
- Если есть базы данных с разной информацией для разных целей, их нельзя объединять;
- Если сведения передают за границу, нужно убедиться, что там есть система защиты такой информации, а сотрудник дал отдельное согласие на передачу данных.



Хранение ПД в электронном виде

Основные правила хранения информации в электронном виде определены в 149-ФЗ от 27.07.2006:

- Серверы размещаются в помещениях с ограниченным доступом работников, имеющих на это право (например, системные администраторы).
- На серверах должно быть установлено защитное программное обеспечение: антивирусы, межсетевые экраны.
- Для защиты ПД выбирают способы исходя из вида данных и уровня защиты, который для них требуется (Приказ ФСТЭК России от 18 февраля 2013 г. N 21).
- Для специальных персональных данных и биометрических требуется 1 или 2 уровень защиты. Это означает, что серверы должны работать надежно, на них нужно установить систему обнаружения вторжений и обязательно создавать резервную копию.
- Для иных данных подходит 3 уровень защиты, можно просто ограничить доступ к системе. Для общедоступных сведений — 4 уровень, достаточно антивирусного приложения.
- Если компания собирается хранить персональные сведения в центре обработки данных ЦОД, то нужно проверить, есть ли у него аттестат на соответствие требованиям приказа ФСТЭК. Это гарантирует, что данные под надежной защитой.



Письменное обязательство о неразглашении персональных данных (п. 43 постановления Пленума Верховного Суда РФ от 17.03.2004 №2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации»)

В Верховный Суд РФ делает акцент на том, что работодателю для применения мер дисциплинарной ответственности за ненадлежащие действия в с ПД необходимо получить письменное обязательство сотрудника не разглашать персональные данные других работников.



Письменное обязательство о неразглашении персональных данных

С должностных лиц, допущенных к ПД, берется **Письменное обязательство о неразглашении персональных данных** работников, в котором фиксируется следующая информация:

- не передавать и не раскрывать третьим лицам полученные конфиденциальные сведения;
- сообщать руководителю предприятия о попытках получить конфиденциальную информацию третьими лицами;
- не использовать персональные данные работников с целью получения какой-либо выгоды;
- при работе с персональными данными работников соответствовать нормативным правовым актам, которые регламентируют вопросы защиты таких сведений.

Обязательство о неразглашении персональных данных – документ, получаемый от тех работников, которые имеют доступ к персональным данным работников предприятия.

Обязательство о неразглашении персональных данных

Я, ----- паспорт серии -----, номер ----- выдан -----,

понимаю, что получаю доступ к персональным данным работников ООО ... Я также понимаю, что во время исполнения своих обязанностей я занимаюсь сбором, обработкой и хранением персональных данных работников.

Я понимаю, что разглашение такого рода информации может нанести ущерб работникам организации, как прямой, так и косвенный.

В связи с этим даю обязательство при работе (сборе, обработке и хранении) с персональными данными сотрудника соблюдать все описанные в Положении о персональных данных требования.

Я подтверждаю, что не имею права разглашать сведения о (об):

- анкетных и биографических данных;
- образовании;
- трудовом и общем стаже;
- составе семьи;
- паспортных данных;
- воинском учете;
- заработной плате работника;
- социальных льготах;
- специальности;
- занимаемой должности;
- наличии судимостей;
- адресе места жительства, домашнем телефоне;
- месте работы или учебы членов семьи и родственников;
- содержании трудового договора;
- составе декларируемых сведений о наличии материальных ценностей;
- содержании декларации, подаваемой в налоговую инспекцию;
- подлинниках и копиях приказов по личному составу;
- личных делах и трудовых книжках сотрудников;
- делах, содержащих материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копиях отчетов, направляемых в органы статистики.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника, или их утраты я несу ответственность в соответствии с ст. 90 ТК РФ.

С Положением о порядке обработки персональных данных работников ООО ... и гарантиях их защиты ознакомлен(а).

специалист по кадрам

(должность)

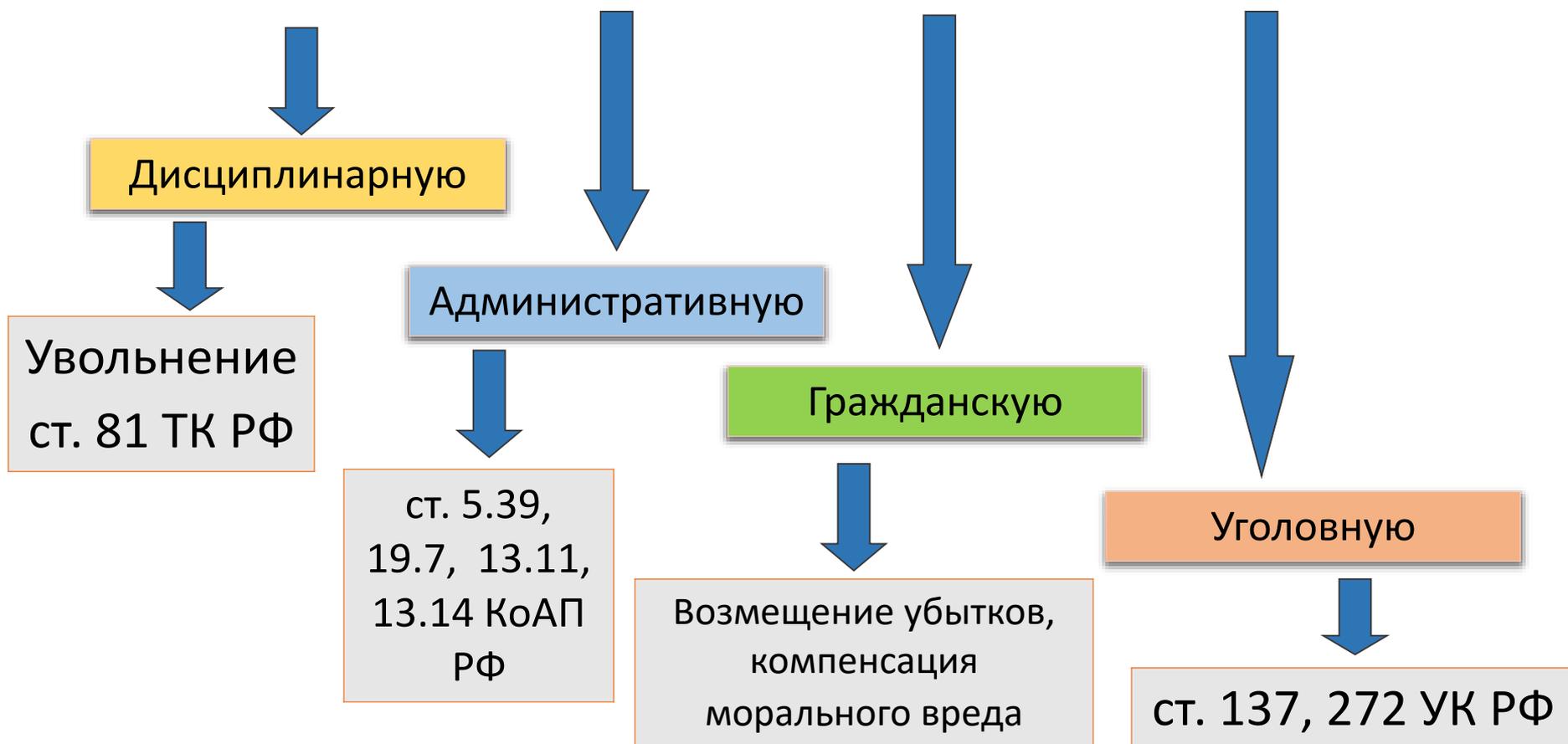
(Ф.И.О.)

«...» _____ 201_ г.



Ответственность оператора за нарушение порядка работы с ПД

Операторы несут ответственность за виновные действия нарушающие требования Закона № 152-ФЗ (ст. 24) :





Пошаговая инструкция «Как организовать хранение персональных сведений в компании»

1. Установить и зафиксировать в Политике (Положении) о ПД порядок доступа в специальное помещение или к местам хранения персональной информации согласно п.13 постановления Правительства от 15.09.2008 № 687.
2. Назначить тех, кто будет обрабатывать ПД и нести за это ответственность. Это могут быть работники кадровой службы или бухгалтерии. Ознакомить работников под подпись с этим документом.
3. Собрать письменные обязательства о нераспространения с лиц, допущенных к ПД.
4. Составить перечень персональных данных, которые будут обрабатывать в организации. В том числе те, которые передают третьим лицам: в ПФР, ГИТ, налоговую или статистику;



Пошаговая инструкция «Как организовать хранение персональных сведений в компании»

5. Заранее разработать формы заявлений о согласии на обработку, хранение и передачу персональных сведений, также журналы учета и проверок — в случае если неожиданно придут проверяющие из Роскомнадзора или ФСТЭК;
6. Выбрать место для хранения персональных данных на бумаге и оформить это приказом.
7. Разработать и утвердить форму обязательства о неразглашении персональных данных и подписать его с сотрудниками, которые отвечают за работу с этой информацией;
8. Подать уведомление в Роскомнадзор о том, что компания является оператором персональных данных, если еще не подали;
9. После необходимо контролировать весь процесс работы с персональными данными, следить за изменениями в законодательстве и периодически проводить независимый аудит.



Ответственный и допущенные к персональным данным

Работодатель обязан своим приказом:

- назначить ответственного за организацию работы с ПД
- утвердить перечень лиц, которых допустили к обработке персональных данных. Это сотрудники, которые работают с ПД работников, клиентов, абонентов и т. д. В приказе укажите, к каким данным имеет доступ конкретный работник.

В должностные инструкции или трудовые договоры работников, допущенных к работе с ПД, включите информацию о том, что они обрабатывают эти данные без использования средств автоматизации. Также укажите, какие категории ПД обрабатывают и какими правилами руководствуются.

ПРИКАЗ № _____

о назначении ответственного за работу
с персональными данными

Руководствуясь статьей 22.1 Закона от 27 июля 2006 г. № 152-ФЗ «О персональных
данных»,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за работу с персональными данными начальника
отдела кадров.
2. На время отсутствия начальника отдела кадров ответственным за работу с
персональными данными является специалист по кадрам.
3. Работнику, указанному в пункте 1 (п. 2) настоящего приказа, осуществлять
установленный режим обработки и защиты персональных данных работников.
4. Контроль над исполнением приказа оставляю за собой.

Директор _____



Что контролирует Роскомнадзор (Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций)?

- Роскомнадзор контролирует работу операторов любых персональных данных (сотрудников или клиентов).
- Подконтрольными субъектами выступают все предприятия, большинство ИП и даже некоторые граждане, которые вне зависимости от объема, обрабатывают и собирают информацию о клиентах, сотрудниках и других гражданах.

У вас есть наемные работники?

Да?! Будьте уверены, вы точно попадаете под проверки Роскомнадзора по персональным данным (ПД)



Роскомнадзор проверяет:

Документы, включающие в себя персональные данные. Если проверка выездная – еще и условия их хранения, организацию места хранения.

Хранение данных на предприятии может быть физическим или электронным.

Роскомнадзор проверяет оба метода:

- Обработывающие их системы (компьютеры и программы);
- Внутренние нормативные акты, касающиеся обработки и хранения персональных данных, и их практическое соблюдение;
- Сайт компании в интернете.

Например, предприятие могут оштрафовать, если на его сайте производится сбор персональных данных (для регистрации нужно вводить свое имя, номер телефона), но не размещены подробности дальнейшей работы компании с персональными данными.



Что проверяет Роскомнадзор:

Единого перечня документов для проверки Роскомнадзором, не существует, но приблизительный список такой:

- Учредительные документы фирмы (свидетельство о государственной регистрации, ИНН, ЕГРЮЛ, устав общества и прочие);
- Копия уведомления о намерении осуществлять работу с персональными данными (можно заменить выпиской из реестра операторов);
- Список персональных данных, собираемых и охраняемых вашей компанией;
- Список сотрудников, имеющих доступ к персональным данным, вместе с приказом об их допуске;
- Инструкции сотрудников, которые в ходе своей трудовой деятельности обрабатывают персональные данные и обеспечивают информационную защиту;
- Политика о ПД (Положение):
Положение об ответственности работников за разглашение персональных данных и нарушение запрета доступа к ним;



Что проверяет Роскомнадзор:

- Положения о коммерческой тайне, о защите персональных данных, хранящихся на предприятии;
- Положения об особенностях обработки персональных данных, в том числе их обезличивания;
- Документы, характеризующие систему защиты персональных данных (план мероприятий, акт определения уровня защищенности);
- Положения, касающиеся информационной безопасности (об антивирусах, паролях, инструктажи сотрудников по требованиям информационной безопасности);
- Соглашения о неразглашении персональных данных, подписанные всеми сотрудниками;
- Бланки согласия граждан на обработку их персональных данных;
- Журналы инструктажей сотрудников по вопросам информационной безопасности и прочих внутренних контрольных мероприятий режима защиты;
- Журналы учета всех носителей информации, а также средств защиты информационных систем.



Основные типы проверок Роскомнадзора

Процедура проверки во многом зависит от ее вида:

Плановые. Их график составляется заранее, еще в конце предыдущего года, и публикуется на сайте. Кроме того, проверяемого предупредят письмом или лично как минимум за три дня до начала инспекции.

Внеплановые. Они инициируются после поступления жалоб от недовольных клиентов или даже от доноса конкурента. В зависимости от серьезности предполагаемого нарушения о проверке могут предупредить за сутки, а могут и не предупредить вовсе.

Документарные. Проверяется пакет документов, который по запросу предоставляется в контролирующий орган.

Выездные. Осматривается территория предприятия.



Ответственность за нарушения

Срок давности

За нарушения по ст. 13.11 КоАП РФ в области ПД могут оштрафовать в течение **1 года**.

Штрафы

1. Незаконная или нецелевая обработка ПД на должностных лиц и ИП – от **10 000 до 20 000** рублей; компании – от **60 000 до 100 000** рублей.

Ранее вместо штрафа можно было отделаться предупреждением. Но теперь такой нормы **нет**.

Ответственность за **повторное** аналогичное нарушение (ч. 1.1. ст. 13.11 КоАП РФ):

для должностных лиц – от **20 000 до 50 000** рублей;
ИП – от **50 000 до 100 000** рублей;
компаний – от **100 000 до 300 000** рублей.



Ответственность за нарушения

Штрафы

2. За обработку ПД без письменного согласия гражданина, если оно **обязательно**, ошибки в содержании согласия, а также за игнорирование требований субъекта ПД (ч. 2 ст. 13.11 КоАП РФ):
должностные лица и ИП – от **20 000 до 40 000** рублей;
компании – от **30 000 до 150 000** рублей.

Ответственность за **повторное** подобное нарушение (ст. 13.11 КоАП РФ):

для должностных лиц – от **40 000 до 100 000** рублей;
ИП – от **100 000 до 300 000** рублей;
компаний – от **300 000 до 500 000** рублей.



Ответственность за нарушения

Штрафы

3. За необеспечение неограниченного доступа к политике обработки персональных данных или к информации о выполняемых требованиях по их защите (ч. 3 ст. 13.11 КоАП РФ):
для должностных лиц – от **6000 до 12 000** рублей;
ИП – от **10 000 до 20 000** рублей;
компаний – от **30 000 до 60 000** рублей.

Ранее штраф можно было заменить предупреждением. Но теперь такой нормы **нет**.



Ответственность за нарушения

Штрафы для интернет-провайдеров за несоблюдение правил безопасности Рунета (ст. 13.42 и др.):

1. За невыполнение порядка установки, эксплуатации и модернизации технических средств борьбы с угрозами российскому сегменту Интернета (ст. 13.42)
2. Для ЮЛ - от 15 000 до 500 000 рублей.
3. За неисполнение владельцем информационного ресурса, причастным к нарушениям основополагающих прав и свобод человека, прав и свобод граждан РФ, предупреждения о необходимости прекращения противоправных действий (ст. 19.7.10-3)
для ЮЛ - до **3-х млн рублей** .



Рекомендации о действиях во время проверки

1. Вы имеете право ознакомиться с документами, относящимися к проверке, с положениями и регламентом;
2. Не экономьте на помощи профессионалов. Даже присутствие юриста придаст вам уверенности и поможет не упустить из виду важных мелочей в переговорах и оформлении документов;
3. Не паникуйте;
4. Тщательно проверяйте документы, прежде чем передать их инспектору. По возможности снимайте со всего копии;
5. Выездной осмотр может проводиться только в присутствии понятых. Если их нет, вы имеете право обжаловать результаты проверки через суд;
6. Инспекторы не имеют права изымать документы, не имеющие отношения к предмету проверки, составляйте опись изымаемых документов;
7. Не предоставляйте требуемые документы мгновенно. Вы имеете право на некоторое время для обработки запроса. Не торопитесь, проверьте все еще раз перед передачей инспектору.



Основной план подготовительных мероприятий к проверке Роскомнадзора

1. Убедитесь, что ранее вы подавали в Роскомнадзор уведомление об обработке персональных данных. Подавать его нужно прежде, чем начинать деятельность, и опоздание уже становится поводом для штрафа. На практике Роскомнадзору почти всегда удается доказать, что каждый работодатель является оператором персональных данных. Какие бы факты он ни приводил в доказательство обратного.
2. Проверьте, соответствует ли ваша текущая деятельность указанному в едином реестре. Уточните содержание заявления, которое вы ранее подавали в Роскомнадзор и при необходимости внесите в него изменения. Необходимую для этого форму можно скачать на сайте Роскомнадзора. Именно несоответствие этих данных и фактической деятельности выступает самой распространенной причиной штрафа от Роскомнадзора. Например, даже назначение другого ответственного за обработку персональных данных сотрудника уже становится основанием для штрафа.

ч.1 ст.22 152-ФЗ:

Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.

Не является исключением!

Обработка персональных данных субъектов (работников, членов семьи работников) поручается третьим лицам.

Размещение на интернет ресурсах форм, позволяющих вносить персональные данные пользователей; РАСПРОСТРАНЕНИЕ - путем размещения сведений на информационных порталах.

Обработка персональных данных акционеров, учредителей, являющихся физическими лицами, индивидуальными предпринимателями.

Ведение баз потенциальных или бывших клиентов с целью информирования о деятельности организации; хранение персональных данных уволненных работников.

ч.2 ст.22 152-ФЗ:

Оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных:

1. Обрабатываемые в соответствии с трудовым законодательством;
2. Обработка ПД, полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются.



Виды деятельности (оквэд), не подпадающие под исключения ч. 2 ст. 22 федерального закона

64.9 (65.2) – деятельность по предоставлению прочих финансовых услуг, кроме услуг по страхованию и пенсионному обеспечению

64.92 (65.22) – предоставление займов и прочих видов кредита

64.92.1 (65.22.1) – деятельность по предоставлению потребительского кредита

64.92.6 (65.22.6) – деятельность по предоставлению ломбардами краткосрочных займов под залог движимого

64.92.7 (65.22) – деятельность микрофинансовая

64.99 (65.23) – предоставление прочих финансовых услуг, кроме услуг по страхованию и пенсионному обеспечению, не включенных в другие группировки

Данные виды деятельности предполагают наличие договорных отношений с потребителями услуг, в рамках которых собираются персональные данные иных лиц (доверенные лица, сведения о поручителях и пр.), при этом напрямую с иными лицами договор не заключается. Например, при подаче онлайн-заявки на кредит в адрес финансовой организации передаются данные третьих лиц, при этом напрямую с ними договор не заключается. Также, предполагается передача персональных данных – потребителей услуг третьим лицам (организации по взысканию задолженности, оценочные компании, страховые компании, бюро кредитных историй). Данный вид деятельности не подпадает под исключения ч. 2 ст. 22 Федерального закона.

[Профилактика
коронавирусной инфекции](#)[Об управлении](#)[Новости](#)[Государственная служба](#)[Планы и отчеты о
деятельности](#)[Конкурсы и тендеры](#)[Правовая информация](#)[Требования к подконтрольным
субъектам](#)[Противодействие коррупции](#)[Массовые коммуникации](#)[Связь](#)[Персональные данные](#)[Нормативно-правовые акты](#)[Условия обработки
персональных данных.
Права субъектов
персональных данных](#)[Ведение реестра операторов,
осуществляющих обработку
персональных данных](#)[Государственный
контроль\(надзор\) за
соответствием обработки
персональных данных
требованиям
законодательства РФ](#)[Образец заполнения
формы уведомления об
обработке \(о намерении
осуществлять обработку\)
персональных данных](#)[Кодекс добросовестных
практик в сети Интернет](#)[Памятки / Презентации](#)[Молодежная палата](#)[Информация для
несовершеннолетних](#)[Главная страница](#) > [Персональные данные](#)

Образец заполнения формы уведомления об обработке (о намерении осуществлять обработку) персональных данных

Образец заполнения формы уведомления об обработке (о намерении осуществлять обработку) персональных данных

Уведомление оформляется на бланке органа, осуществляющего обработку персональных данных.

Уведомлению присваивается номер и указывается дата составления.

Подаваемый документ (оригинал) обязательно подписывается уполномоченным лицом (руководителем)

Руководителю Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Иркутской области

С.Е. Костылову

ул. Халтурина, д. 7, а/я 169
г. Иркутск, 664011

[Уведомление об обработке](#)

(о намерении осуществлять обработку) персональных данных

1. Тип оператора:

- **Тип оператора:** юридическое лицо/государственный или муниципальный орган/индивидуальный предприниматель/физическое лицо (указать что-либо одно).
- **Полное и сокращенное наименования Оператора с указанием организационно-правовой формы:** Общество с ограниченной ответственностью "Первый" (ООО "Первый")
- **Фамилия, имя, отчество Оператора:** Индивидуальный предприниматель Иванов Иван Иванович (ИП Иванов И.И.).
- **Паспорт серия** ___ № ___ **выдан** _____ **дата выдачи** _____ **(заполняется только индивидуальными предпринимателями и физическими лицами)**
- **Адрес регистрации:** 664000, Иркутская обл., г. Иркутск, ул. Первая, д. 1, оф. 1 (указываются в строгом соответствии со свидетельством о постановке юридического лица на учет в налоговом органе).
- **Почтовый адрес:** 664000, Иркутская обл., г. Иркутск, а/я 1 (если совпадает с адресом регистрации, заполнять не обязательно)
- **ИНН:** 3800000000
- **ОГРН:** 0000000000000
- **наименование филиала (представительства) юридического лица (при наличии):** Филиал ООО "Первый", находящийся по адресу: 630000, Новосибирская обл., г. Новосибирск, ул. Новая, д. 1

2. Цель обработки персональных данных:

Необходимо указать как цели, указанные в учредительных документах (уставе, учредительном договоре, положении) оператора, так и цели фактически осуществляемой оператором деятельности.

Например:

- «осуществление трудовых взаимоотношений с работниками...»,
- «осуществление видов деятельности в соответствии с Уставом...»,



Основной план подготовительных мероприятий

3. Назначьте ответственного за обработку персональных данных, вместе с ним приступайте к подготовке всех документов, сопровождающих путь персональных данных от сбора, до хранения и уничтожения.
4. Обязательно оформите «Политику компании в отношении обработки персональных данных». Вы можете дать документу другое название, но суть в том, что он станет основополагающим сводом правил и инструкций в интересующем Роскомнадзор вопросе.
5. Подготовьте к проверке всех сотрудников. Ознакомьте их с документами по работе с персональными данными. Установите четкие правила поведения с инспекторами, если ожидается выездная проверка. Очень часто у проверяющих возникают вопросы к простым работникам. Отработайте с ними тактику «глухой защиты» – ничего не говорить, ничего не подписывать без присутствия руководителя. Вы имеете на это право.



Основной план подготовительных мероприятий

6. Проверьте, как и где вы храните бумаги, особенно ксерокопии паспортов, кто имеет к ним доступ.
7. Проверьте материально-техническое оснащение офиса: замки на важных помещениях, наличие сейфов для документов.
8. Воспользуйтесь специальными онлайн-сервисами для подготовки документов. Они бывают совсем бесплатными или коммерческими, но в любом случае дешевле офлайн специалиста. Особенно если вы практически не знакомы с законодательством о персональных данных, сервисы дадут исключительно актуальные подсказки по подготовке.



10 основных ошибок в работе с ПД, за которые штрафует Роскомнадзор

1. Собираем и храним лишние документы
2. Не проводим внутренний аудит работы с ПД
3. Не опубликована политика обработки ПД
4. Не утвержден перечень лиц, имеющих доступ к ПД
5. Работники не ознакомлены под подпись с законом о ПД
6. Используем неверный бланк согласия на обработку ПД
7. Неправильно заполнено уведомление об обработке ПД
8. Не сообщили в Роскомнадзор, что изменили сведения, которые указали в уведомлении
9. Не назначен ответственный за обработку ПД
10. Не утвержден перечень мест хранения ПД



1. Собираем и храним лишние документы

Запрещено хранить лишние документы, которые содержат персональные данные сотрудников. В группе риска копии паспортов, дипломов и свидетельств и другие бумаги с информацией о сотруднике.

Как избежать претензий?

1. Продумайте состав личных дел. Следите за их содержанием.
2. Оригиналы документов храните в отдельных папках по тематике или в соответствии со сроками их хранения.
3. Дополнительные документы храните в отдельной папке под замком.
4. Уничтожайте ненужные документы с ПД вовремя.
5. Разбирайте документы уволившихся.



Хранение копий документов

Хранение в личных делах работников копий, содержащих ПД, **не является нарушением закона, ЕСЛИ** работодатель обеспечил одновременное соблюдение следующих условий:

1. от работника получено согласие на хранение его ПД, указанных в копиях документов, необходимость обработки которых не обусловлена достижением целей, поименованных в п.п. 2-11 ч. 1 ст. 6 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных";
2. Работодателем заранее определены конкретные цели хранения персональных данных, содержащихся в копиях документов работников, при этом такие цели не противоречат законодательству;
3. объем персональных данных, указанных в копиях документов работника, не превышает необходимый объем данных для использования в соответствии с заявленными целями обработки.

Если эти условия не соблюдаются (например, хранение копий личных документов работника не обусловлено необходимостью достижения конкретных, заранее определенных и законных целей обработки ПД), хранение копий таких документов неправомерно.



2. Не проводим внутренний аудит работы с ПД

п. 4 ч. 1 ст. 18.1 Закона от 27.07.2006 № 152-ФЗ

Компания обязана проводить внутренний аудит работы с ПД.

Как избежать претензий?

1. Разработайте положение о внутреннем аудите.
2. Ознакомьте с ним работников.
3. Составьте план аудита.
4. Создайте комиссию, которая будет его проводить.
5. Состав комиссии утвердите приказом.
6. По итогам аудита комиссия должна оформлять заключительный документ — акт или протокол. В нем необходимо:
 - проанализировать работу с ПД
 - выдать рекомендации по улучшению процессов с ПД.



3. Не опубликована политика обработки ПД

ч. 2 ст. 18.1 Закона от 27.07.2006 № 152-ФЗ

Компания должна издать и опубликовать (или иным образом обеспечить неограниченный доступ) политику обработки ПД.

Как избежать претензий?

1. Разработайте политику или актуализируйте ее по Рекомендациям Роскомнадзора от 27.07.2017.
2. Не копируйте формулировки ведомства, ориентируйтесь на специфику вашей организации.
3. Опубликуйте политику на сайте компании. Если его нет, сделайте документ в бумажном виде доступным для всех заинтересованных лиц. Например, при входе и т. п.
4. Если сайтов несколько, разместите политику на всех. Роскомнадзор это проверяет. По функционалу сайтов текст делить не нужно.



4. Не утвержден перечень лиц, имеющих доступ к ПД

ст. 88 ТК РФ.

Работодатель должен приказом утвердить перечень сотрудников, которые в связи с исполнением должностных обязанностей имеют доступ к ПД. Получать они должны только те данные, которые им нужны, чтобы выполнять конкретные трудовые функции.

Как избежать претензий?

1. Издайте приказ об утверждении перечня лиц, имеющих доступ к ПД. Обычно в перечень входят генеральный директор, его заместители, работники кадровой службы, бухгалтерии, службы безопасности, юридического отдела и т. д.
2. Лучше указать не ФИО конкретных работников, а список должностей, чтобы не вносить изменения в приказ при приеме и увольнении работников.
3. Предусмотрите нем, об дисциплинарной, административной или уголовной ответственности за разглашение ПД.
4. Ознакомьте всех допущенных к ПД работников с приказом под подпись.



5. Работники не ознакомлены под подпись с законом о ПД

п. 6 ч. 1 ст. 18.1 Закона от 27.07.2006 № 152-ФЗ

Работников необходимо ознакомить с положениями законодательства о персональных данных.

Как избежать претензий?

1. Оформите лист ознакомления работников с положениями законодательства о персональных данных и внутренними документами по вопросам обработки персональных данных.
2. Другой вариант — включите положения в трудовой договор с работником.
3. Знакомить работников с документами в электронном виде рискованно. В Роскомнадзоре считают, что в этом случае работодатель не выполняет свою обязанность надлежащим образом.



6. Используем неверный бланк согласия на обработку ПД

ч. 4 ст. 9 Закона от 27.07.2006 № 152-ФЗ

Согласие на обработку персональных данных должно включать все обязательные реквизиты.

Роскомнадзор в форме согласия обычно находит четыре ошибки:

- не указали адрес или данные паспорта работника;
- не указали перечень ПД, на обработку которых компания получает согласие;
- не указали способ, как работник может отозвать согласие;
- указали несколько целей обработки персональных данных.

Как избежать претензий?

1. Разработайте шаблон согласия или внесите изменения в существующий.
2. Не получайте у работника универсальное согласие на все случаи (отдельный документ под каждую цель) Например, на рассмотрение кандидата, включая запрос рекомендаций у прежнего работодателя, передачу сведений в банк, и тп



7. Неправильно заполнено уведомление об обработке ПД

ч.1 ст.22 Закона от 27.07.2006 № 152-ФЗ

Компания должна уведомить территориальный орган Роскомнадзора о том, что будет обрабатывать ПД.

Как избежать претензий?

1. Чтобы внести в уведомление полные сведения, изучите устав, локальные акты, договоры и согласия на обработку ПД.
2. Не скачивайте готовый образец заполненного уведомления из интернета. Он не подходит — надо учитывать специфику компании.
3. Будете составлять уведомление, используйте Методические рекомендации Роскомнадзора, утв. приказом от 30.05.2017 № 94,.



Характерные ошибки в уведомлении

1. Цель обработки ПД:
Указывается информация несоответствующая целям обработки (например, в целях реализации Федерального закона № 152-ФЗ).
2. Правовое основание: Ссылка только на Федеральный закон № 152-ФЗ; Не вписываются отраслевые НПА.
3. Категории персональных данных:
Указываются не все категории ПД;
Допускаются фразы «и др.», «и т.п.», «другая информация».
4. Категории субъектов ПД:
Указываются не все категории субъектов ПД (например, родственники, члены семьи, кандидаты и др.)
5. Перечень действий с ПД, способы обработки:
Не указывается конкретный перечень действий с ПД;
Отсутствует либо не четко указан порядок передачи информации при или автоматизированной обработке.



Характерные ошибки в уведомлении

6. Описание мер, предусмотренных ст. 18.1 и 19 закона № 152-ФЗ:

- Организационные и технические меры не раскрываются;
- При смешанной обработке не указывается отдельно перечень мер по обеспечению безопасности;
- Не указывается использование средств шифрования, криптографической защиты информации.

7. Ответственный за организацию обработки ПД:

- необходимо указать либо наименование и контактные данные **иного юридического лица**, либо фамилию, имя, отчество **Вашего** сотрудника, ответственных за организацию обработки персональных данных, а также контактные данные).

8. Сведения об обеспечении безопасности ПД:

Необходимо указать сведения и меры принятых юридическим лицом в целях исполнения требований установленных Постановлением Правительства РФ от 15.09.2008 № 687 и Постановлением Правительства РФ от 01 ноября 2012 г. № 1119



8. Не сообщили в Роскомнадзор, что изменили сведения, которые указали в уведомлении

ч. 7 ст. 22 Закона от 27.07.2006 № 152-ФЗ

Если сведения, указанные в уведомлении о начале обработки ПД изменились, в Роскомнадзор нужно направить письмо. Например, поменялся перечень обрабатываемых ПД, категории субъектов, назначили нового ответственного за организацию обработки ПД и т. п. Срок отправки письма — 10 рабочих дней.

Как избежать претензий?

1. Форма информационного письма есть в Приложении № 2 к Рекомендациям № 94. Она практически такая же, как форма уведомления.
2. Заполните те поля, в которых изменяются сведения. Внесите данные о компании и укажите территориальный орган Роскомнадзора, куда направяете письмо.
3. Информационное письмо можно передать лично, направить почтой, в электронном виде через единый портал Госуслуг, на сайте Роскомнадзора.
4. В 30-дневный срок Роскомнадзор рассмотрит письмо и внесет изменения в реестр операторов персональных данных.
5. п. 4.2 Рекомендаций № 94. Информацию о внесении сведений размещают на сайте и Портале персональных данных Роскомнадзора.



9. Не назначен ответственный за обработку ПД

п. 4 ч. 1 ст. 18.1 , ч. 2 ст. 22.1 Закона от 27.07.2006 № 152-ФЗ

Необходимо назначить одного ответственного за организацию работы с ПД, даже когда штат большой и есть филиальная сеть. Ответственный должен подчиняться напрямую генеральному директору и иметь полномочия давать указания руководителям подразделений.

Роскомнадзор не рекомендует назначать кадровика или бухгалтера ответственным за организацию работы с ПД, если речь не идет о маленьких компаниях.

Как избежать претензий?

1. Назначьте ответственным директора по персоналу или по информационной безопасности, они подчиняются напрямую руководителю организации, обладают достаточными знаниями.
2. Проследите, что ответственному дали достаточно полномочий.
3. О назначении ответственного издайте приказ в произвольной форме.
4. Пропишите подробно полномочия в трудовом договоре или должностной инструкции.



10. Не утвержден перечень мест хранения ПД

Необходимо в ЛНА или приказе утвердить перечень мест хранения материальных носителей ПД (дела, папки, журналы и т. д.)

В помещениях, где обрабатываются ПД на бумаге, определите места хранения — сейфы или запираемые шкафы. Местом хранения может быть и само помещение, например архив компании.

Как избежать претензий?

1. Утвердите приказом перечень мест, где храните материальные носители персональных данных.

Общество с ограниченной ответственностью «Каскад»
(ООО «Каскад»)

ПРИКАЗ

07.08.2019

№ 20

Москва

Об утверждении перечня мест хранения материальных носителей персональных данных

С целью исполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных в ООО «Каскад»

ПРИКАЗЫВАЮ:

1. Определить перечень мест хранения персональных данных, обрабатываемых в ООО «Каскад» (Приложение 1).
2. Ознакомить сотрудников, допущенных к обработке персональных данных, с перечнем мест хранения.
3. Контроль за исполнением настоящего приказа возложить на ответственного за организацию обработки персональных данных Иванову П.Р.

Генеральный директор

Максимов

А.М. Максимов

С приказом ознакомлены:

...

Приложение 1

ПЕРЕЧЕНЬ
мест хранения материальных носителей персональных данных

№ п/п	Подразделение	Место нахождения	Наименование документа, содержащего персональные данные
1	Отдел кадров	Ул. Живописная, 123, кабинет 1, шкаф, сейф	Личные карточки сотрудников, трудовые книжки, приказы по личному составу, трудовые договоры
2	Бухгалтерия	Ул. Живописная, 123, кабинет 2, шкаф	Индивидуальные сведения о трудовом стаже, зарплатке (вознаграждении), доходе и начисленных страховых взносах застрахованного лица, расчетные (расчетно-платежные) ведомости; листки нетрудоспособности
3	...		

Татьяна
Костерина



HR - грамотные решения

КОНТАКТЫ

Костерина Татьяна Анатольевна, hr-эксперт



+7 (910) 994 90 37



t.a.costerina@gmail.com



<https://hr37.ru>



https://t.me/tatyana_kosterina_hr37





Дистанционные и выездные услуги Т.А.Костериной по вопросам работы с персоналом:



**КОНСУЛЬТАЦИИ, УСЛУГИ ПО АУДИТУ
СОБЛЮДЕНИЮ ТРУДОВОГО
ЗАКОНОДАТЕЛЬСТВА, ПОДГОТОВКА К
ПРОВЕРКАМ ГИТ, ОБУЧЕНИЕ,
РЕГЛАМЕНТАЦИЯ РАБОТЫ КАДРОВЫХ
СЛУЖБ, РАЗРАБОТКА И РЕАЛИЗАЦИЯ
СТРАТЕГИЙ РАБОТЫ С ПЕРСОНАЛОМ, СХЕМ
МОТИВАЦИИ**

Запись на установочную(бесплатную) консультацию можно:

- на сайте <https://hr37.ru>
- в Telegram, WhatsApp, Viber , телефон - +7(910) 994-90-37
- по электронной почте - t.a.costerina@gmail.com

ВАШЕ СПОКОЙСТВИЕ – МОЯ РАБОТА!

Случаи, когда обрабатывать персональные данные можно без согласия работника (Разъяснение Роскомнадзора от 14.12.2012)

Обязанность обрабатывать персональные данные работников, в том числе публиковать и размещать их в интернете, предусматривает закон

Сведения о родственниках работника не превышают объем, предусмотренный формой № Т-2, или требуются в особых случаях — получение алиментов, оформление социальных выплат

Работодатель обрабатывает сведения о состоянии здоровья работника, которые нужны для выполнения трудовой функции

Данные передаются третьим лицам при исполнении должностных обязанностей (например, командировка) или для предупреждения угрозы жизни и здоровью

Сведения работников направляют в ФСС, ПФР, налоговые органы, военные комиссариаты, профсоюзные органы

Получен мотивированный запрос от правоохранительных органов и прокуратуры, органов безопасности, инспекторов ГИТ

Работодатель самостоятельно организует пропускной режим на территорию служебных зданий и помещений

**Обязательные реквизиты согласия работника
на обработку персональных данных**

**Ф. И. О., адрес работника, номер документа,
удостоверяющего личность, дата его выдачи и выдавший орган**

Наименование работодателя

Цель обработки персональных данных

**Перечень персональных данных, на обработку
которых работник дает согласие**

**Перечень действий с персональными данными, на совершение которых
работник дает согласие, общее описание способов обработки данных**

Срок, в течение которого действует согласие, а также способ его отзыва

Подпись работника