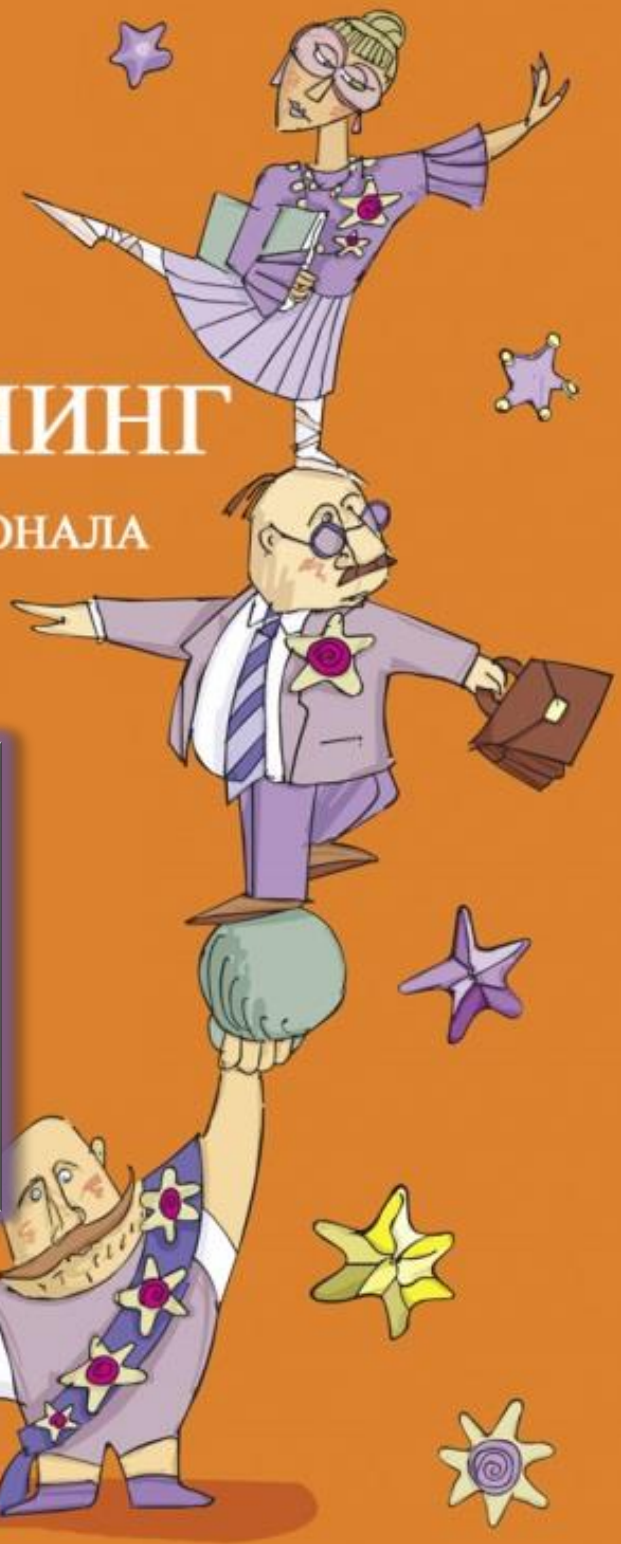
КонсультантПлюс



СЕМИНАР-ТРЕНИНГ

ПРАКТИКУМ ДЛЯ ПРОФЕССИОНАЛА



Персональные данные: что необходимо учесть кадровику в 2022-2023 гг.

420021, г. Казань, ул. Татарстан, 22. 8 этаж
Тел: 8-800-700-52-23 (843)515-20-20
E-mail: cons@vkons.ru
Сайт: vkons.ru

Оглавление

1. Изменения и перспективы 2022-2023 гг.……...……....3

2. Персональные данные как составная часть конфиденциальной информации о работниках……..……14

3. Обязанности работодателя по защите персональных данных работников при их обработке и хранении ……...33

4. Порядок организации работ по обеспечению безопасности персональных данных работников при обработке и хранении ……...37

5. Ответственность за нарушение норм законодательства о персональных данных……..…42

Вопрос №1. Изменения и перспективы 2022-2023 гг.

Нормативные акты:

1. *Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных" {КонсультантПлюс}*
2. *Федеральный закон от 14.07.2022 N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" {КонсультантПлюс}*
3. *Федеральный закон от 28.05.2022 N 145-ФЗ "О внесении изменения в статью 14.8 Кодекса Российской Федерации об административных правонарушениях" {КонсультантПлюс}*
4. *Федеральный закон от 01.05.2022 N 135-ФЗ "О внесении изменения в статью 16 Закона Российской Федерации "О защите прав потребителей" {КонсультантПлюс}*
5. *Приказ Роскомнадзора от 05.08.2022 N 128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных" {КонсультантПлюс}*

Содержание вопроса:

1. Основные изменения в Законе о персданных
2. Уведомление об обработке персональных данных
3. Локальные акты по вопросам обработки персональных данных
4. Согласие на обработку персональных данных
5. Новые запреты
6. Поручение по обработке персданных
7. К кому требования о распространении персданных не относятся
8. Биометрические персданные
9. Трансграничная передача персданных
10. Взаимодействие с ГосСОПКА
11. Новые сроки
12. Чем подтвердить факт удаления персональных данных?

Защита персональных данных в настоящий момент приобрела приоритетное значение. Поэтому в спешном порядке были подготовлены и приняты поправки в Закон о персданных, большинство из которых вступили в силу с сентября 2022 года. Следующая "порция" заработает в марте 2023 года. У работодателей появились новые обязанности, законодатели сократили ряд сроков, ввели очередные запреты для операторов персданных. Изменения коснулись широкого круга вопросов. Среди них: когда нужно уведомить о намерении обрабатывать персональные данные; что включать в локальные акты и как их правильно размещать на сайте компании; что делать, если

произошла утечка данных.

На сегодняшнем вебинаре проанализируем новшества и расскажем, на что обратить внимание работодателям, операторам персданных и рядовым гражданам.

Основные изменения в Законе о персданных

По новым правилам нормы Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон N 125-ФЗ) следует применять в том числе и к обработке персданных граждан РФ, осуществляемой иностранными юридическими и физическими лицами как по договору, так и на основании согласия гражданина на эту обработку. Другими словами, независимо от конкретного вида обработки данных. Если обработку данных им будет поручать российский оператор, то он будет нести ответственность за их действия наравне с ними (ч. 1.1 ст. 1 и ч. 6 ст. 6 Закона N 152-ФЗ).

Теперь с Роскомнадзором должны быть согласованы все нормативные правовые акты РФ, затрагивающие вопросы:

- трансграничной передачи персональных данных;
- обработки специальных категорий данных (например, состояние здоровья человека);
- биометрических данных;
- персональных данных несовершеннолетних лиц;
- а также вопросы предоставления и распространения персональных данных, полученных в результате обезличивания.

У ведомства по Закону будет 30 дней на согласование проекта документа.

Уведомление об обработке персональных данных

1. Из Закона о персональных данных исключили большинство случаев, когда компаниям не нужно было уведомлять Роскомнадзор о намерении начать обрабатывать персональные данные.

Таким образом, следует проинформировать ведомство, если компания собирается обрабатывать, в частности, персональные данные (ссылки ведут на утратившие силу нормы о случаях, когда уведомление не требовалось):

- своих работников;
- клиентов (когда данные о них нужны исключительно для заключения и исполнения договоров);
- физлиц, которые разрешили их распространять;
- физлиц - только в части Ф.И.О.;
- физлиц - для однократного пропуска на территорию или в аналогичных целях.

Если для обработки персональных данных не используют средства автоматизации, уведомлять ведомство не нужно. Например, данные о посетителях организации записывают в бумажный журнал при выдаче им разовых пропусков.

Роскомнадзор указал: уведомление нужно подать также и тем, кто уже обрабатывал персональные данные в ситуациях, которые ранее считались исключением. Крайний срок подачи уведомления не определен.

2. Скорректировали требования к содержанию уведомления. Если данные будут обрабатывать в разных целях, то **для каждой из них** понадобится указать:

- категорию данных и их субъектов;
- правовое основание обработки;
- перечень действий с данными и способы их обработки.

Если у физлиц или юрлиц есть доступ к персональным данным в государственных (муниципальных) информационных системах или они обрабатывают данные из этих систем по договору, Ф.И.О. таких физлиц (наименование юрлиц) нужно привести в уведомлении.

3. В законе закрепили положение о том, что формы уведомлений должен установить Роскомнадзор (пока действует рекомендуемая форма, которую можно заполнить и подать через портал персональных данных (https://pd.rkn.gov.ru/operators-registry/notification/)).

Локальные акты по вопросам обработки персональных данных

В законе конкретизировали требование о том, что локальные акты должны содержать:

- категории и перечни обрабатываемых данных;
- категории субъектов данных;
- способы и сроки обработки, хранения данных;
- порядок их уничтожения.

Эти положения нужно установить для каждой цели обработки данных.

Если компания собирает персональные данные граждан через свой сайт, проверьте, где именно на сайте опубликован документ о политике обработки данных и сведения о реализуемых компанией требованиях к их защите.

Такая информация должна быть опубликована в том числе на страницах сайта, где непосредственно идет сбор персональных данных (например, на страницах с формами, которые заполняют пользователи).

Согласие на обработку персональных данных

В число требований к согласию включили то, что оно должно быть предметным и однозначным.

Если получение согласия обязательно, компания должна разъяснить физлицу последствия не только отказа в предоставлении данных, но и отказа дать согласие на их обработку.

Цель поправок - усиление защиты субъектов персональных данных и обеспечение неприкосновенности их частной жизни. Дело в том, что в последнее время появилось множество сервисов в Интернете, которые незаконно собирают, хранят и распространяют персональную

информацию о гражданах, включая паспортные данные, сведения о недвижимости, перелетах и иные личные сведения. В частности, деанонимизация, влекущая раскрытие персональных данных военнослужащих и их семей, создает непосредственную угрозу их жизни и безопасности в текущих непростых условиях.

Более того, нелегальные сервисы, как правило, расположены за пределами РФ и потому не подпадают под ее юрисдикцию. Трансграничная передача персданных нашими законами практически не регулируется, а осуществляется большим количеством операторов повсеместно и в больших масштабах.

Рассмотрим подробнее, какие меры ввело государство для защиты персональных данных и что это значит для работодателей, операторов персданных и рядовых граждан.

Новые запреты

В договор с субъектом персональных данных нельзя включать следующие условия (п. 5 ч. 1 ст. 6 Закона N 152-ФЗ):

- ограничивающие его права и свободы. Например, на отзыв согласия на обработку персданных или соблюдение дополнительных условий для такого отзыва, включая значительный срок, за который нужно подать уведомление оператору;
- устанавливающие случаи обработки персданных несовершеннолетних лиц, если иное не предусмотрено законодательством РФ;
- допускающие в качестве условия заключения договора бездействие субъекта персональных данных. Скажем, у оператора может возникнуть соблазн не получать отдельное согласие от гражданина, а включить условие о заранее данном согласии в оферту, к которой тот присоединяется в целом, оговорив, что, если он не согласен с таким условием, он должен проставить соответствующее обозначение. Раньше в договорах банковского вклада некоторые банки нередко включали условие, что при несогласии вкладчика с обработкой его персональных данных, включая биометрические, он должен прямо об этом в договоре написать, в ином случае согласие считается полученным. Теперь так делать нельзя.

Поручение по обработке персданных

Новая редакция ч. 3 ст. 6 Закона N 152-ФЗ более детально регламентирует вопросы поручения оператором обработки персданных субъектов иным лицам, в том числе государственным и муниципальным органам власти. Лицо, которому поручается обработка, должно обеспечить базовые принципы обработки данных, их конфиденциальность, принимать меры к выполнению всех своих обязанностей.

Справочно. В мае этого года Минцифры согласовало оборотные штрафы за утечку данных

пользователей. Законопроект предусматривает введение оборотных штрафов в 1% в случае утечки и в 3% в случае, если компания скрыла инцидент. Теперь в законопроект внесли уточнения - власти откажутся от оборотных штрафов за утечки, если они касаются менее 10 000 человек. Но за такие нарушения все равно придется отвечать. Правда, компаниям грозит не оборотный, а фиксированный штраф.

В самом поручении на обработку нужно определить:
- перечень данных;
- перечень действий по их обработке;
- цели и иные обязательные требования;
- право оператора и корреспондирующую обязанность лица, которому поручается обработка, предоставлять документы и информацию, подтверждающие выполнение обязательных требований.

Естественно, оператору не стоит ограничиваться только поручением, а рекомендуется заключить договор и оформить соответствующие отношения как обязательства, включив в него в том числе штрафы за нарушения в соответствии со ст. 330 ГК РФ.

Также на случай нарушения контрагентом условий договора можно предусмотреть, что он в качестве имущественных потерь возместит все суммы штрафов, компенсаций и иных расходов и других убытков, которые возникнут в связи с предъявлением требований со стороны субъектов персональных данных и контролирующих органов (ст. 406.1 ГК РФ). Такое договорное условие позволит вашей организации как оператору персданных создать источник возмещения за счет контрагента-нарушителя, учитывая, что от рисков неправильных действий (бездействия) в отношении персданных сейчас никто не застрахован.

К кому требования о распространении персданных не относятся

Требования ст. 10.1 Закона N 152-ФЗ об особенностях обработки персданных путем распространения теперь не будут касаться не только государственных и муниципальных органов, но и подведомственных им организаций (ч. 15 указанной статьи).

Поправка логична, учитывая, что не все свои властные полномочия и функции органы власти осуществляют самостоятельно. Для этих целей они создают и используют подведомственные организации. В ином же случае деятельность органов власти была бы существенно затруднена дополнительными формальностями, связанными с необходимостью получения согласия от субъекта персональных данных и организацией этого процесса.

Биометрические персданные

Согласно новой ч. 3 ст. 11 Закона N 152-ФЗ получение биометрических персональных данных

обязательным не является. Подобное уточнение совсем не лишнее, учитывая, что банки и иные профессиональные участники рынка их собирают (достаточно вспомнить, как при открытии счета в банке клиентов фотографируют), но при этом многие из них, к сожалению, так и не научились должным образом их защищать (в новостях информация о масштабных "сливах" персданных появляется чуть ли не еженедельно).

Поэтому граждане теперь могут отказываться предоставлять биометрические данные. А организация будет не вправе на этом основании отказать в заключении договора. Такой отказ будет считаться незаконным (см. также информацию на сайте Минцифры России (https://digital.gov.ru/ru/events/41802/)).

Трансграничная передача персданных

С 1 марта 2023 года ст. 12 Закона N 152-ФЗ о трансграничной передаче персональных данных начнет действовать в новой редакции. По новым правилам, придется ориентироваться на перечень иностранных государств, которые обеспечивают адекватную защиту прав субъектов персональных данных, такой перечень будет формировать и вести Роскомнадзор.

Справочно. В марте 2021 года вступили в силу изменения, связанные с использованием персональных данных граждан путем их распространения среди неопределенного круга лиц. Нововведения касаются в том числе и работодателей, которые так или иначе раскрывают персональные данные работников для неограниченного круга. Например: компания размещает на своем официальном сайте или иных информационных сайтах информацию о своих довольных клиентах с историями об оказанной им услуге или сделанной работе либо организация-работодатель в разделе "Наша команда" собственного сайта указывает краткую информацию о своих работниках с их фотографиями и контактной информацией и пр. Ситуации довольно распространенные. Форма согласия на распространение таких персданных не утверждена, однако ее содержание можно определить на основании требований ст. 10.1 Закона о персданных и Приказа Роскомнадзора N 18. Самое главное - согласие на распространение таких персональных данных оформляется отдельно от иных согласий.

Кроме того, до начала трансграничной передачи данных о своем намерении это делать нужно будет уведомить Роскомнадзор. Если какие-то организации осуществляют трансграничную передачу уже сейчас, такое уведомление им необходимо направить в ведомство до 1 марта 2023 года. Уведомление придется подавать отдельным документом, а не вместе с общим уведомлением о намерении осуществлять обработку персональных данных. Это сделано для того, чтобы вовремя вмешаться и предотвратить возможные нарушения прав субъектов персональных данных. Очевидно, что в большом потоке входящей информации Роскомнадзор не сможет оперативно

выявлять нужные уведомления.

Наиболее сложным нововведением является требование к оператору до подачи уведомления получить от органов власти иностранных государств, иностранных физических или юридических лиц сведения:

- о принимаемых мерах по защите прав субъектов персональных данных;
- о правовом регулировании персданных в иностранном государстве;
- об органах власти иностранного государства, иностранных юридических и физических лицах, которым будут передаваться данные.

Причем Роскомнадзор может принять отказное решение, запрещающее трансграничную передачу данных, в целях защиты основ конституционного строя, безопасности жизни и здоровья граждан, а также в иных значимых целях. На принятие решения чиновникам дается 10 рабочих дней (с момента поступления уведомления). При положительном решении регулятора оператор может осуществлять трансграничную передачу персданных на тех территориях и в том объеме, которые указаны в решении Роскомнадзора. Вполне очевидно, что до принятия соответствующего решения оператор этим заниматься не вправе, поскольку с марта начинает действовать разрешительный, а не уведомительный порядок.

Рекомендации в связи с изменениями можно дать следующие:

1. включите в локальные акты положения о порядке получения и документирования оператором от органов иностранного государства, иностранных физлиц или юрлиц, которым планируется трансграничная передача ПД, сведений, предусмотренных ч. 5 ст. 12 Закона № 152-ФЗ. Это сведения:

- о мерах по защите передаваемых ПД и об условиях прекращения их обработки, принимаемых иностранными лицами, которым планируется трансграничная передача ПД;
- о правовом регулировании в области ПД иностранного государства, под юрисдикцией которого находятся иностранные лица, которым планируется трансграничная передача ПД (если предполагается передача ПД иностранным лицам, находящимся под юрисдикцией иностранного государства, не являющегося стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и не включенного в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПД);
- об иностранных лицах, которым планируется трансграничная передача ПД (наименование либо ФИО, а также номера контактных телефонов, почтовые адреса и адреса электронной почты);

2. включите в локальные акты положения о проведении оператором оценки соблюдения иностранными лицами, которым планируется трансграничная передача ПД, конфиденциальности ПД и обеспечения безопасности ПД при их обработке;

3. проанализируйте и при необходимости скорректируйте существующую практику трансграничной передачи ПД и получения согласия на предмет ее оптимизации (то есть для

сокращения количества случаев трансграничной передачи ПД и уменьшения числа получателей ПД в «неадекватных» юрисдикциях);

4. после анализа запросите у оставшихся актуальными зарубежных получателей ПД сведения, предусмотренные ч. 5 ст. 12 Закона № 152-ФЗ;

5. после запроса сведений у иностранных лиц уведомите Роскомнадзор о намерении осуществлять трансграничную передачу ПД;

6. проанализируйте и доработайте типовые формы договоров об обработке ПД и зарепите в них механизм уничтожения ПД их зарубежными получателями в случае принятия Роскомнадзором соответствующего решения. Внесите изменения в уже заключенные договоры;

7. отслеживайте процесс принятия проекта нового приказа Роскомнадзора «Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных».

Взаимодействие с ГосСОПКА

На оператора теперь возложена обязанность обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ - ГосСОПКА (см. ст. 5 Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"), включая информирование о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных (ч. 12 ст. 19 Закона N 152-ФЗ).

Порядок такого взаимодействия будет определен органом власти, уполномоченным в сфере обеспечения безопасности (видимо, имеется в виду МВД РФ). Такая мера позволяет повысить гарантии информационной безопасности нашей страны в целом за счет эффективной и слаженной защиты всех ее информационных элементов на самых различных уровнях, а также позволяет более плотно вовлечь операторов в юридически значимые для органов власти процессы.

Раз оператор как предприниматель зарабатывает в нашей стране, в том числе на использовании персональной информации граждан, он должен более ответственно, а не формально подходить и к вопросам ее защиты. Более того, он сам непосредственно участвует в обработке персональных данных, поэтому может и обязан незамедлительно сигнализировать о возможных нарушениях и инцидентах, а не делать вид, что они его не касаются.

Обратите внимание! Оператор должен предоставить субъекту возможность определить перечень персональных данных по каждой категории, указанной в согласии на обработку персональных данных, разрешенных гражданином для распространения. В документе должны быть указаны: Ф.И.О., контактная информация субъекта (телефон, электронная почта или почтовый адрес); сведения об операторе (наименование, адрес из ЕГРЮЛ, ИНН, ОГРН 3) и его информационных

ресурсах (например: https://... http://www...); цели обработки персональных данных, их категории и перечень с выделением тех данных, для которых предусматриваются особые условия и запреты, связанные с обработкой, а также срок действия согласия.

Новые сроки

Оператору персональных данных стоит иметь в виду, что с 1 сентября сокращаются с 30 до 10 рабочих дней сроки некоторых действий (ч. 1, 2, 4 ст. 20 Закона N 152-ФЗ). Так, оператору в этот период необходимо:

- ответить на обращение субъекта персональных данных по поводу того, обрабатывает ли он его данные, и если да, то предоставить к ним доступ;
- дать мотивированный ответ об отказе предоставить информацию о наличии обрабатываемых персданных;
- сообщить Роскомнадзору необходимые сведения по его запросу.

Кроме того, у оператора появились новые обязанности по уведомлению Роскомнадзора (ч. 3.1 ст. 21 Закона N 152-ФЗ). При выявлении случаев неправомерной или случайной передачи персданных оператор обязан:

- в течение 24 часов с момента обнаружения такого нарушения уведомить ведомство об инциденте, его причинах, предполагаемом вреде субъекту персданных, принятых мерах, уполномоченном лице, которое от имени оператора взаимодействует с ведомством;
- в течение 72 часов сообщить ведомству о результатах внутреннего расследования, а также направить сведения о лицах, действия которых стали причиной инцидента.

Справочно. Минцифры начало обсуждать с некоторыми IT-компаниями возможность создания фонда материальной компенсации для граждан, чьи персональные данные утекли из баз данных. Как предполагается, средства для фонда будут поступать от оборотных штрафов, которые компании обяжут выплачивать за утечки данных, указал источник в крупной российской IT-компании.

При обращении субъекта персданных к оператору с требованием прекратить их обработку последний обязан это сделать в течение 10 рабочих дней. Этот срок может быть продлен, но не более чем на пять рабочих дней, при этом придется направить гражданину мотивированное уведомление с указанием причин такой меры (ч. 5.1 ст. 21 Закон N 152-ФЗ). Невыполнение данных требований будет свидетельствовать о нарушении закона со стороны оператора, в связи с чем Роскомнадзор может его привлечь к административной ответственности по ст. 13.11 КоАП РФ.

Чем подтвердить факт удаления персональных данных?

Персональные данные нужно уничтожать, если они собраны незаконно, если достигнуты цели их сбора и если этого требует сам владелец данных. Роскомнадзор разработал проект приказа (опубликован на Федеральном портале проектов нормативных правовых актов), в котором установил требования к уничтожению персональных данных.

Уничтожение персональных данных означает уничтожение документов, в которых эти данные хранятся. Бумажные документы могут быть сожжены, измельчены на шредере и т.п. Электронные - удалены, затерты и т.п.

Как правило, персональные данные хранятся с момента их получения до момента, когда утрачена цель их обработки. После этого в течение 30 дней персональные данные должны быть уничтожены (ч. 4, 5 ст. 21 Закона N 152-ФЗ). Кроме того, сами работники, в первую очередь уволенные, могут потребовать прекратить хранение их персональных данных.

В каких случаях персональные данные нужно уничтожить:

- их обработали неправомерно (ч. 3 ст. 21 Закона N 152-ФЗ);
- достигнуты цели, ради которых компания собирала и обрабатывала данные (ч. 4 ст. 21 Закона N 152-ФЗ);
- владелец данных требует уничтожить их (ч. 1 ст. 14, ч. 3 ст. 20 Закона N 152-ФЗ);
- владелец данных отзывает согласие на обработку данных (ч. 5 ст. 21 Закона N 152-ФЗ).

Самым распространенным документом фиксации факта уничтожения персональных данных является акт о прекращении обработки персональных данных либо запись об этом факте в специальном журнале. Делает это специально созданная комиссия по уничтожению персональных данных.

Процедура уничтожения персданных состоит из трех этапов:

- издание приказа и создание комиссии;
- уничтожение персональных данных;
- составление акта об уничтожении ПД.

Обратите внимание! Требования указать в согласии паспортные данные и адрес регистрации субъекта нет. Поэтому их можно в согласие не включать, если вы их не знаете и у гражданина нет намерения вам их представлять. Вместе с тем если такие данные у вас есть, то их целесообразно в согласие включить, поскольку обязанность доказывать законность распространения персданных лежит на операторе, осуществившем их распространение. А значит, чем лучше у вас составлены документы, тем проще вам будет доказать законность своих действий в случае возникновения спора или претензий со стороны контролеров. В Приказе Роскомнадзора N 18 персональные данные разделены на три категории. Рекомендуем именно так указать их в согласии, чтобы гражданин мог выбрать, какие сведения он разрешает о себе распространять неограниченному

кругу лиц, а какие нет.

Акт уничтожения персональных данных - это самый важный документ, в котором фиксируется сам факт уничтожения персональных данных. Роскомнадзор разработал приказ, которым устанавливаются требования к акту.

Акт об уничтожении персональных данных должен содержать:

- наименование или Ф.И.О. (при наличии) и адрес оператора;
- наименование или Ф.И.О. (при наличии), адрес лица, осуществляющего обработку персональных данных субъекта персональных данных по поручению оператора (если обработка поручена такому лицу);
- Ф.И.О. (при наличии) субъекта или иную информацию, относящуюся к определенному физическому лицу, чьи персональные данные были уничтожены;
- Ф.И.О. (при наличии), должности лиц, уничтоживших персональные данные субъекта персональных данных, а также их подписи;
- перечень уничтоженных персональных данных;
- наименование уничтоженного материального носителя, содержащего персональные данные, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта персональных данных (в случае обработки персональных данных с использованием средств автоматизации);
- способ уничтожения персональных данных;
- причину уничтожения персональных данных;
- дату уничтожения персональных данных.

Акт может быть оформлен на бумаге или в электронном формате.

Если персональные данные обрабатывались в собственной электронной системе или БД, нужно составить акт уничтожения и выгрузку данных из журнала регистрации событий в информационной системе персональных данных.

Файл должен содержать:

- Ф.И.О. (при наличии) субъекта или иную информацию, относящуюся к определенному физическому лиц;
- перечень уничтоженных данных;
- причину уничтожения персональных данных.

Вопрос №2. Персональные данные как составная часть конфиденциальной информации о работниках

Нормативные акты:

1. *Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных" {КонсультантПлюс}*
2. *Федеральный закон от 14.07.2022 N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" {КонсультантПлюс}*
3. *Федеральный закон от 28.05.2022 N 145-ФЗ "О внесении изменения в статью 14.8 Кодекса Российской Федерации об административных правонарушениях" {КонсультантПлюс}*
4. *Федеральный закон от 01.05.2022 N 135-ФЗ "О внесении изменения в статью 16 Закона Российской Федерации "О защите прав потребителей" {КонсультантПлюс}*
5. *Приказ Роскомнадзора от 05.08.2022 N 128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных" {КонсультантПлюс}*
6. *Указание Банка России от 16.12.2021 N 6017-У "О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой" {КонсультантПлюс}*

Содержание вопроса:

1. Что относится к персональным данным и какие документы их содержат?
2. Как получить персональные данные работника?
3. Нужно ли получать согласие работника на обработку персональных данных?
4. Нужно ли и как уведомлять Роскомнадзор об обработке персональных данных сотрудников?
5. Какие общие требования закона учитывать при обработке персональных данных работников организации?
6. В каких целях могут обрабатываться персональные данные работника?
7. Какие документы о порядке обработки персональных данных должны быть в организации?
8. Порядок обработки персональных данных без использования средств автоматизации
9. Порядок обработки персональных данных с использованием средств автоматизации
10. Организация учета и хранения персональных данных
11. Изменение персональных данных
12. Передача персональных данных сотрудника

Что относится к персональным данным и какие документы их содержат?

Персональными данными является любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу. Персональные данные могут быть разрешенными для распространения (ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных)).

К персональным данным относятся:

- фамилия, имя, отчество;
- пол, возраст;
- образование, квалификация, профессиональная подготовка и сведения о повышении квалификации;
- место жительства;
- семейное положение, наличие детей, родственные связи;
- факты биографии и предыдущая трудовая деятельность (место работы, судимость, служба в армии, работа на выборных должностях, на государственной службе и др.);
- финансовое положение. Сведения о заработной плате также являются персональными данными (Письмо Роскомнадзора от 07.02.2014 N 08КМ-3681);
- деловые и иные личные качества, которые носят оценочный характер;
- прочие сведения, которые могут идентифицировать человека.

Из указанного списка работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора. Подробнее об этом см. п. 2 настоящего материала.

В процессе трудовой деятельности работника работодатель копит и хранит документы, содержащие персональные данные работника. Исходя из определения персональных данных, которое дано в ст. 3 Закона о персональных данных, такие сведения могут содержаться в следующих документах:

- анкета, автобиография, личный листок по учету кадров, которые заполняются работником при приеме на работу. В этих документах содержатся анкетные и биографические данные работника;
- копия документа, удостоверяющего личность работника. Здесь указываются фамилия, имя, отчество, дата рождения, адрес регистрации, семейное положение, состав семьи работника, а также реквизиты этого документа;
- личная карточка N Т-2. В ней указываются фамилия, имя, отчество работника, место его рождения, состав семьи, образование, а также данные документа, удостоверяющего личность, и пр.;
- трудовая книжка или ее копия. Содержит сведения о трудовом стаже, предыдущих местах работы;
- сведения о трудовой деятельности (формы СЗВ-ТД, СТД-ПФР, СТД-Р). Содержат информацию о

местах работы и др.;

- копии свидетельств о заключении брака, рождении детей. Такие документы содержат сведения о составе семьи, которые могут понадобиться работодателю для предоставления работнику определенных льгот, предусмотренных трудовым и налоговым законодательством;
- документы воинского учета. Содержат информацию об отношении работника к воинской обязанности и необходимы работодателю для осуществления в организации воинского учета работников;
- справка о доходах с предыдущего места работы. Нужна работодателю для предоставления работнику определенных льгот и компенсаций в соответствии с налоговым законодательством;
- документы об образовании. Подтверждают квалификацию работника, обосновывают занятие определенной должности;
- документы обязательного пенсионного страхования. Нужны работодателю для уплаты за работника соответствующих взносов;
- трудовой договор. В нем содержатся, в частности, такие персональные данные работника, как фамилия, имя и отчество, дата рождения, место жительства, сведения о документах, удостоверяющих личность, сведения о заработной плате. Кроме того, договор содержит сведения о должности работника, месте работы, рабочем месте;
- подлинники и копии приказов по личному составу. В них содержится информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности работника;
- при необходимости - иные документы, содержащие персональные данные работников.

Кроме того, работодатель в процессе своей деятельности собирает информацию о соискателях, необходимую для принятия решения о вступлении с ними в трудовые отношения. Если эта информация содержит персональные данные соискателей, к ней в полной мере относятся установленные законом требования о сборе, обработке, хранении, защите персональных данных.

Как получить персональные данные работника?

Все персональные данные работника получайте только у него самого (п. 3 ст. 86 ТК РФ). Если получить у работника персональные данные нельзя, то можно получить их у третьих лиц, соблюдая определенные требования, о которых мы расскажем ниже.

Как получить персональные данные работника у третьих лиц?

Уведомьте работника об этом заранее и получите его письменное согласие (п. 3 ст. 86 ТК РФ).

Оформите такое уведомление письменно, включите в него информацию, указанную в п. 3 ст. 86 ТК РФ:

- цели получения персональных данных работника у третьих лиц;
- предполагаемые источники информации (лица, у которых будете запрашивать данные);
- способы получения данных, их характер;

- возможные последствия отказа работника дать согласие на получение его персональных данных у третьих лиц.

Желательно вручить такое уведомление работнику под подпись, чтобы у вас было доказательство, что он действительно был уведомлен.

Согласие оформите отдельным документом. Рекомендуем оформить его так же, как согласие на обработку персональных данных, с учетом требований ч. 4 ст. 9 Закона о персональных данных. Оно должно включать, в частности:

- Ф.И.О., адрес работника, реквизиты паспорта или иного документа, удостоверяющего его личность, кем и когда выдан;
- наименование и адрес вашей организации;
- перечень персональных данных, на получение которых дает согласие работник;
- срок, в течение которого действует согласие.

Убедитесь, что работник подписал документ. Тогда при необходимости вы докажете, что работник действительно дал вам согласие на получение своих персональных данных у третьей стороны.

Нужно ли получать согласие работника на обработку персональных данных?

Вы вправе обрабатывать персональные данные работника только с его письменного согласия (п. 1 ч. 1 ст. 6, абз. 1 ч. 4 ст. 9 Закона о персональных данных). Уже при приеме на работу оформите согласие работника на обработку персональных данных. Можно сделать отдельный документ или включить условие о согласии в трудовой договор. Обратите внимание, что с 1 сентября согласие на обработку персональных данных должно быть «предметным» и «однозначным» (ч. 1 ст. 9 Закона №152-ФЗ). Это указано в дополнение к тому, что согласие должно быть конкретным, информированным и сознательным.

Срок действия согласия закон не ограничивает, поэтому можно указать любой срок. Например, до дня его отзыва (ст. 9 Закона N 152-ФЗ).

Согласие на обработку персональных данных

Генеральному директору ООО "Альфа"
Иванову И.И.
от бригадира цеха N 1 Петрова П.П.

Согласие
на обработку персональных данных

Я, Петров Петр Петрович (паспорт 45 13 356201, выдан 23.05.2013 отделением УФМС России по г. Москве по району Обручевский, место жительства - г. Москва, ул. Профсоюзная, д. 94, кв. 56), в соответствии со ст. 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" даю свое согласие работодателю - ООО "Альфа" (ОГРН 1127785195230, ИНН 7722345678, адрес - г. Москва, шоссе Энтузиастов, д. 9) на обработку, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение, следующих персональных данных в документальной и/или электронной форме:

1) фамилия, имя, отчество;
2) дата и место рождения;
3) пол;
4) гражданство;
5) паспортные данные;
6) адрес места жительства;
7) семейное положение и сведения о членах семьи;
8) номер телефона, адрес электронной почты;
9) идентификационный номер налогоплательщика;
10) номер страхового свидетельства государственного пенсионного страхования;
11) сведения о воинском учете;
12) фотография;
13) сведения об образовании;
14) сведения о владении иностранными языками;
15) сведения о месте работы, в том числе о предыдущих;
16) размер зарплаты;
17) сведения о состоянии здоровья, связанные с возможностью выполнения трудовой функции.

Согласие дается мною для следующих целей:

1. обеспечение соблюдения законов и иных нормативных правовых актов;
2. предоставление сведений кредитной организации для открытия счета, оформления банковской карты и перечисления зарплаты и других выплат;
3. предоставление сведений страховым организациям для заключения договора добровольного страхования со мной в качестве застрахованного;
4. предоставление сведений работникам ООО "Альфа" и третьим лицам, необходимых для выполнения моей трудовой функции.

Настоящее согласие действует со дня его подписания до дня его отзыва мною в письменной

форме.

Петров
05.09.2022

В частности, вам потребуется получить у работника письменное согласие для размещения его фотографии на Доске почета. Это связано с тем, что фотография является биометрическими персональными данными, то есть сведениями, характеризующими физиологические и биологические особенности человека, на основе которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных. Обработка таких данных работника допустима только при наличии его письменного согласия. Это следует из ст. 88 ТК РФ, ч. 1 и 3 ст. 11 Закона о персональных данных, Письма Роскомнадзора от 10.02.2020 N 08АП-6782.

Исключения прямо регламентированы законом, а также указаны в Разъяснениях Роскомнадзора. Например, не нужно получать такое согласие, если вы организуете пропускной режим на территории вашего здания (абз. 1 п. 5 Разъяснений Роскомнадзора). Или сообщаете персональные данные работника третьей стороне, когда это необходимо в целях предупреждения угрозы его жизни и здоровью (ст. 88 ТК РФ, п. 4 Разъяснений Роскомнадзора).

Нужно ли и как уведомлять Роскомнадзор об обработке персональных данных сотрудников?

Компании и ИП, которые обрабатывают персональные данные, должны соблюдать правила обработки, однако не всем нужно уведомлять Роскомнадзор о том, что она ведется. До 1 сентября 2022 года действовал прежний обширный список случаев, когда можно не уведомлять Роскомнадзор (поправки введены Федеральным законом от 14.07.2022 №266-ФЗ). Однако после этой даты он резко сократился (п. 22 Закона №152-ФЗ в редакции Федерального закона от 14.07.2022 №266-ФЗ).

Так, с 1 сентября 2022 года можно не уведомлять Роскомнадзор об обработке персональных данных, только если:

1. персональные данные включены в государственные электронные ресурсы, которые созданы для защиты безопасности государства и общественного порядка;
2. оператор обрабатывает персональные данные исключительно без использования средств автоматизации, то есть на бумаге;
3. это предусмотрено законами о транспортной безопасности, для обеспечения безопасности транспортного комплекса государства, защиты общества в этой сфере.

Таким образом, работодатели являются операторами персональных данных и с 01.09.2022 обязаны уведомлять Роскомнадзор о начале обработки персональных данных работников. Организациям,

еще не включенным в реестр операторов персональных данных, нужно направить уведомление об обработке персональных данных. А тем, кто уже есть в реестре, нужно уведомить Роскомнадзор о новой цели обработки персональных данных - обработке в рамках трудовых отношений (ст. 22 Закона N 152-ФЗ, Письмо Роскомнадзора от 06.09.2022 N 08-80975).

Специальные формы уведомлений будут утверждены приказом Роскомнадзора. До этого оператор вправе заполнить форму уведомления об обработке персональных данных на Портале персональных данных Роскомнадзора или направить такое уведомление в адрес территориального управления ведомства по месту регистрации оператора на бумажном носителе по форме, утвержденной Приказом от 30.05.2017 N 94.

На портале Роскомнадзора оператору предоставлена возможность сформировать и отправить уведомление в территориальный орган Роскомнадзора одним из следующих способов:

1. в бумажном виде;
2. в электронном виде с использованием усиленной квалифицированной электронной подписи;
3. в электронном виде с использованием средств аутентификации ЕСИА.

После вступления в силу приказа Роскомнадзора, устанавливающего новую форму уведомления, оператор может направить уведомление о внесении изменений в ранее представленные сведения в Реестр операторов, осуществляющих обработку персональных данных.

Предельный срок уведомления Роскомнадзора об обработке персональных данных не определен. Таким образом, 1 сентября 2022 не является крайним сроком подачи уведомления об обработке персональных данных.

Какие общие требования закона учитывать при обработке персональных данных работников организации?

Все общие требования к обработке персональных данных работников установлены ст. 86 ТК РФ. К самым ключевым относятся следующие (подробнее о них расскажем ниже):

- обрабатывайте персональные данные только в определенных целях (например, для трудоустройства работника) (п. 1 ст. 86 ТК РФ);
- получайте персональные данные исключительно у работника. Если их возможно получить только у третьих лиц, сообщите об этом работнику и заручитесь его письменным согласием (п. 3 ст. 86 ТК РФ);
- ознакомьте работников под подпись с локальными нормативными актами, устанавливающими порядок обработки персональных данных (п. 8 ст. 86 ТК РФ);
- вырабатывайте совместно с работниками меры по защите персональных данных (п. 10 ст. 86 ТК РФ).

Кроме того, отдельные требования установлены Законом о персональных данных, в частности:

- до начала обработки персональных данных вы обязаны уведомить Роскомнадзор о

намерении их обрабатывать (ч. 1 ст. 22 Закона о персональных данных);

- если вы установили, что такие данные неправомерно или случайно переданы (предоставлены, распространены и т.д.) и это нарушило права работника, вы обязаны уведомить Роскомнадзор. В течение 24 часов нужно сообщить об инциденте, его причинах, предполагаемом вреде, принятых мерах по устранению последствий и о лице, уполномоченном взаимодействовать с ведомством по данному инциденту. О результатах внутреннего расследования происшествия и лицах, из-за которых оно произошло (если они есть), надо уведомить в течение 72 часов (ч. 3.1 ст. 21 Закона о персональных данных). Формы уведомлений размещены на сайте Роскомнадзора (Информация Роскомнадзора).

В каких целях могут обрабатываться персональные данные работника?

Обрабатывать персональные данные работников можно только в строго определенных целях. Они раскрыты в п. 1 ст. 86 ТК РФ.

Так, обрабатывать персональные данные работника нужно, чтобы:

1) обеспечить соблюдение законов и других нормативных правовых актов (например, передача персональных данных работников в ФСС РФ, ПФР по запросу);

2) помочь работникам в трудоустройстве, получении ими образования, карьерном продвижении (например, при направлении на повышение квалификации);

3) обеспечить безопасность работников, контроль над выполняемой ими работой;

4) обеспечить сохранность имущества.

Например, для безопасности работников, сохранности имущества может вводиться видеонаблюдение.

Какие документы о порядке обработки персональных данных должны быть в организации?

Если компания или ИП не собирает никакие данные физических лиц, то она не является оператором. Например, если у ИП нет работников и он работает только с юридическими лицами и при этом не собирает и не хранит никаких данных физических лиц (допустим, ФИО курьеров). В этом случае можно не оформлять документы, связанные с обработкой персональных данных. Если в компании или у ИП есть работники, значит, они обрабатывают персональные данные.

Конкретный перечень документов, регламентирующих порядок обработки персональных данных работников, законом не установлен.

Как правило, организации издают **положение о персональных данных** или иной локальный нормативный акт по вопросам их обработки. В таком документе описывают все связанные с ней действия (хранение, использование данных и т.д.). Для каждой цели обработки документ должен определять в том числе категории и перечень персональных данных, способы, сроки их обработки и хранения и др. (ст. 87 ТК РФ, п. 2 ч. 1 ст. 18.1 Закона о персональных данных).

Также создайте **документ, определяющий политику в отношении обработки персональных данных** (п. 2 ч. 1 ст. 18.1 Закона о персональных данных). Его структуру и содержание вы можете установить самостоятельно (Письмо Роскомнадзора от 19.10.2021 N 08-71063). При этом целесообразно руководствоваться Рекомендациями, изданными Роскомнадзором.

Такой документ должен включать в себя, в частности, сведения о цели сбора персональных данных, правовых основаниях их обработки, объеме и категориях обрабатываемых данных, порядке и условиях их обработки.

Если у вас нет документа, определяющего политику в отношении обработки персональных данных, разработайте и утвердите его (п. 2 ч. 1 ст. 18.1 Закона о персональных данных).

Вот примерный список документов, которые должен иметь оператор персональных данных. Он составлен исходя из рекомендаций Роскомнадзора и собственного опыта в данной сфере (ссылки указаны на Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»).

Документы:

1. уведомление об обработке персональных данных. Его нужно отправить в Роскомнадзор в момент начала обработки (п. 22 Закона №152-ФЗ);

2. приказ о назначении ответственного за организацию обработки персональных данных у оператора (подп. 1 ч. 1 ст. 18.1, ч. 1 ст. 22.1 Закона №152-ФЗ);

3. формы согласий и сами согласия субъектов персональных данных на обработку персональных данных (ст. 9 Закона №152-ФЗ);

4. политика (положение) об обработке персональных данных (ч. 2 ст. 18.1 Закона №152-ФЗ). При составлении положения можно взять за основу рекомендации Роскомнадзора;

5. документы, описывающие меры, предпринимаемые для защиты персональных данных. Они могут включать:

- инструкцию по контролю доступа в помещения, где проводится обработка персональных данных;
- инструкцию по парольной защите;
- инструкцию по антивирусной защите;
- инструкцию по порядку разрешительного доступа к персональным данным;
- положение о хранении носителей, содержащих персональных данные. Такими носителями могут быть флешка, диск, бумага;
- список помещений, где обрабатываются персональные данные;
- перечень средств защиты информации. В нем указываются названия средств защиты, их количество, производитель и информация о наличии сертификатов ФСТЭК и ФСБ (Постановление Правительства РФ от 01.11.2012 №1119, п. 8.12 Приказа ФСТЭК России от 18.02.2013 №21, подп. 2 ч. 2 ст. 19 Закона №152-ФЗ);

6. положение об обработке обращений и запросов, поступивших от субъектов персональных

данных (п. 3 ч. 4 ст. 22.1 Закона №152-ФЗ). Его можно включить в политику об обработке персональных данных;

7. документ, устанавливающий требования к ведению журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта. Необходим, если в компании пропускной режим (п. 8 Постановления Правительства РФ от 15.09.2008 №687);

8. документ о классификации информационных систем. Например, информационными системами являются:

- 1С, в которой обрабатываются данные по сотрудникам, клиентам (в систему могут подгружать счета, договоры с клиентами);
- сайт, на котором есть форма обратной связи с клиентом, и др.

При классификации информационных систем нужно учитывать:

- Приказ ФСТЭК России от 18.02.2013 №21;
- Приказ ФСТЭК России от 11.02.2013 №17 (для госучреждений);
- Постановление Правительства РФ от 01.11.2012 №1119;

9. список лиц, которым необходим доступ к персональным данным (п. «в» ст. 13 Постановления Правительства от 01.11.2012 №1119, п. 8 ч. 2 ст. 19 Закона №152-ФЗ);

10. положение об обработке персональных данных работников;

11. обязательства работников о неразглашении персональных данных (ст. 90 ТК РФ);

12. модели угроз. В этом документе указывается, как именно стоит защищать данные, какие угрозы со стороны злоумышленников возможны в отношении данных и т. д. Его обязательно нужно составлять на каждую информационную систему, в которой производится обработка персональных данных.

Для подготовки этого документа нужно учитывать:

- Постановление Правительства РФ от 01.11.2012 №1119;
- Методику оценки угроз безопасности информации, утв. ФСТЭК 05.02.2021;
- Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. ФСТЭК 15.02.2008.

Данный перечень включает основные документы, которые должны быть у оператора персональных данных. Также могут быть и другие документы, например:

1. журнал учета проверок контролирующими органами (Роскомнадзором);
2. поручение на обработку персональных данных, если ПД передаются другим лицам (ч. 3 ст. 6 Закона №152-ФЗ). Например, при передаче компании, которая ведет бухгалтерию на аутсорсинге.

Как ознакомить работников с документами о порядке обработки персональных данных в организации?

Ознакомьте работников с документами, которые у вас в организации регламентируют порядок

обработки персональных данных, под подпись (п. 8 ст. 86, ч. 2 ст. 22 ТК РФ).

Вы можете использовать такой же порядок ознакомления, что и при ознакомлении с Правилами внутреннего трудового распорядка (например, с помощью листа ознакомления, составленного в свободной форме).

А документ, определяющий политику в отношении обработки персональных данных, дополнительно опубликуйте (ч. 2 ст. 18.1 Закона о персональных данных). Например, разместите на сайте организации.

Если это сделать невозможно, нужно сделать политику доступной каким-то иным способом (ч. 2 ст. 18.1 Закона о персональных данных). Например, повесьте распечатанную на бумаге политику на стенде в офисе. Главное, обеспечьте неограниченный доступ к документу (Письмо Роскомнадзора от 19.10.2021 N 08-71063).

Порядок обработки персональных данных без использования средств автоматизации

Согласно п. 3 ст. 4 Закона о персональных данных порядок обработки персональных данных, осуществляемой без использования средств автоматизации, может устанавливаться федеральными законами и иными нормативными правовыми актами РФ.

В настоящее время действует Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства РФ от 15.09.2008 N 687 (далее - Положение). Согласно данному Положению обработкой персональных данных без применения средств автоматизации считаются использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, которые осуществляются при непосредственном участии человека (п. 1 Положения, утвержденного Постановлением Правительства РФ от 15.09.2008 N 687). Соответственно, если персональные данные работников обрабатываются в компьютерной (информационной) системе, это не означает, что данная обработка производится с помощью средств автоматизации (п. 2 Положения). Таким образом, к обработке персональных данных работников в организации должны применяться правила, предусмотренные для обработки данных без использования средств автоматизации.

Персональные данные при такой обработке должны быть обособлены от иной информации, в частности, путем фиксации их на отдельных материальных носителях.

Согласно п. 6 Положения лица, осуществляющие обработку персональных данных без использования средств автоматизации (в т.ч. сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте такой обработки, категориях обрабатываемых данных, а также об особенностях и правилах такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, а также локальными

правовыми актами организации (при их наличии).

Пункт 7 Положения содержит условия, которые необходимо соблюдать при использовании типовых форм документов, предполагающих или допускающих включение в них персональных данных, например унифицированных форм первичной учетной документации по учету труда и его оплаты, утвержденных Постановлением Госкомстата России от 05.01.2004 N 1.

Согласно пп. "а" п. 7 Положения типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать: сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации; фамилию, имя, отчество и адрес оператора; фамилию, имя, отчество и адрес субъекта персональных данных; источник получения данных; сроки их обработки; перечень действий с персональными данными, которые будут совершаться в процессе их обработки; общее описание используемых оператором способов обработки персональных данных.

Типовая форма должна содержать поле, в котором субъект персональных данных может проставить отметку о согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения такого согласия (пп. "б" п. 7 Положения).

При этом форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими данными, не нарушая прав и законных интересов иных субъектов персональных данных (пп. "в" п. 7 Положения). Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы (пп. "г" п. 7 Положения).

Порядок обработки персональных данных с использованием средств автоматизации

Согласно ст. 3 Закона о персональных данных под автоматизированной обработкой понимается обработка данных с помощью средств вычислительной техники. Необходимо учитывать, что обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что эти данные содержались в информационной системе персональных данных либо были извлечены из нее (п. 2 Положения).

Персональные данные работников обрабатывает уполномоченный на это представитель работодателя. Следовательно, он должен руководствоваться правилами, предусмотренными для обработки персональных данных без использования средств автоматизации.

Организация учета и хранения персональных данных

Согласно п. 7 ст. 86 ТК РФ защиту персональных данных работника от неправомерного их использования или утраты работодатель должен обеспечивать за счет своих средств. В

соответствии со ст. 87 ТК РФ порядок хранения и использования персональных данных работников устанавливается работодателем. Из данных норм следует, что работодатель должен издать соответствующий локальный нормативный акт, регулирующий вопросы хранения и использования персональных данных, а также обеспечивающий защиту последних от неправомерного их использования или утраты. С соответствующим актом, а также со своими правами в сфере защиты персональных данных работники должны быть ознакомлены под подпись.

Пунктом 10 ст. 86 ТК РФ предусмотрено, что работодатели и их представители должны совместно вырабатывать меры защиты персональных данных работников. Подробнее об этом см. п. 4 настоящего материала.

Ситуация из практики. **Можно ли хранить копии документов в личном деле работника?**

Хранить копии документов (паспорта, СНИЛС, трудовой книжки) работника в его личном деле работодатель может, если работник дал согласие на хранение и обработку персональных данных (Доклад с руководством по соблюдению обязательных требований, дающих разъяснение, какое поведение является правомерным, а также разъяснение новых требований нормативных правовых актов за II квартал 2017 г. (утв. Рострудом)).

Вместе с тем Роскомнадзор считает такое хранение обработкой персональных данных, избыточных по отношению к заявленным целям обработки, что нарушает ч. 5 ст. 5 Закона N 152-ФЗ. Аналогичной позиции придерживаются суды. Так, в Постановлениях Пятнадцатого арбитражного апелляционного суда от 14.03.2014 N 15АП-22502/2013 по делу N А53-12557/2013, ФАС Северо-Кавказского округа от 21.04.2014 по делу N А53-13327/2013 указано, что собирая и храня в документах кадрового учета копии страниц паспорта, военного билета и других документов, которые содержат персональные данные работника, организация превысила объем обрабатываемых персональных данных.

Учитывая неоднозначность позиции по рассматриваемому вопросу, рекомендуем не хранить в личных делах работников документы, содержащие их персональные данные, если такая необходимость не установлена нормативно. Это позволит избежать ответственности по ч. 1 - 2.1 ст. 13.11 КоАП РФ.

Ситуация из практики. **Как организовать хранение персональных данных, содержащихся в документах личного дела работника?**

Работодателю необходимо установить порядок хранения персональных данных, содержащихся в документах. Возможность и порядок такого хранения нужно отразить в

локальных нормативных актах, касающихся хранения и использования персональных данных. Работников и их представителей с локальными актами нужно ознакомить под подпись (п. п. 7, 8 ст. 86, ст. 87 ТК РФ).

Поскольку на работодателя возложена обязанность соблюдать режим конфиденциальности персональных данных, то целесообразно вести журналы учета персональных данных, их выдачи и передачи другим лицам и представителям различных организаций, государственным органам.

В журнале учета внутреннего доступа к персональным данным (доступа работников организации к персональным данным других работников) следует указывать такие сведения, как дата выдачи и возврата документов (личных дел), срок пользования, цели выдачи, наименование выдаваемых документов (личных дел). Лицо, которое возвращает документ (дело), должно обязательно присутствовать при проверке наличия всех имеющихся документов по описи, если выданные документы составлены более чем на одном листе.

Лицо, которое получает личное дело другого работника во временное пользование, не имеет права делать в нем какие-либо пометки, исправления, вносить новые записи, извлекать документы из личного дела или помещать в него новые.

Помимо этого, также следует вести журнал учета выдачи персональных данных работников организациям и государственным органам, в котором необходимо регистрировать поступающие запросы, а также фиксировать сведения о лице, направившем запрос, дату передачи персональных данных или уведомления об отказе в их предоставлении и отмечать, какая именно информация была передана.

Система учета персональных данных также может предусматривать проведение регулярных проверок наличия документов и других носителей информации, содержащих персональные данные работников, а также устанавливать порядок работы с ними. В этой связи необходимо ведение журнала проверок наличия документов, содержащих персональные данные работника.

Работодатель обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных работников от неправомерного использования или утраты либо обеспечить принятие таких мер. Это следует из п. 7 ст. 86 ТК РФ, ч. 1 ст. 19 Закона о персональных данных.

В частности, работодатель может предусмотреть в локальном нормативном акте требования к помещениям, в которых находятся носители информации (например, компьютеры с базами данных, документы на бумажных носителях), содержащие персональные данные работников.

Обращаем внимание, что Закон о персональных данных и Трудовой кодекс РФ не устанавливают каких-либо требований к упомянутым помещениям. Представляется, что работодатель может определить особый режим доступа в них, требования к оборудованию, установить перечень лиц,

имеющих право доступа в данные помещения. Такие выводы следуют из анализа ч. 1, 2 ст. 19 Закона о персональных данных, ч. 1 ст. 8, абз. 7 ч. 1 ст. 22, ст. 87 ТК РФ.

Исходя из п. 21 Методических рекомендаций по ведению воинского учета в организациях (утв. Минобороны России 11.07.2017) документы воинского учета, содержащие персональные данные работников, рекомендуем хранить в железных шкафах в специально оборудованных помещениях.

В соответствии со ст. 88 ТК РФ работодатель обязан не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью последнего, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами.

Однако возникают случаи, когда отдельным работникам нужно получить информацию о персональных данных других работников, которые они намереваются использовать при выполнении трудовых обязанностей. Например, бухгалтеру могут понадобиться данные о работнике для начисления ему заработной платы или уплаты соответствующих взносов, при направлении работников в командировку секретарю (или иному лицу) понадобятся паспортные данные последних для покупки билетов, юрисконсульту организации данные работников могут понадобиться для оформления доверенностей и т.д. В соответствии со ст. 88 ТК РФ работодатель может разрешить доступ к персональным данным работников только специально уполномоченным лицам, при этом указанным лицам будут доступны только те данные, которые необходимы для выполнения конкретных функций. Например, доступ к персональным данным работников обычно устанавливается для руководителя организации, руководителей структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения), руководителю нового подразделения - при переводе сотрудника из одного структурного подразделения в другое, работникам бухгалтерии и отдела кадров. Конкретный перечень работников, которые имеют доступ к персональным данным других работников, должен быть установлен локальным нормативным актом организации и приказом организации.

Изменение персональных данных

Законом не предусмотрена обязанность работника своевременно уведомлять работодателя об изменении своих персональных данных.

Однако несвоевременное предоставление работником измененных данных может повлиять на исполнение работодателем своих обязанностей. Поэтому в Положении об обработке и защите персональных данных целесообразно зафиксировать обязанность работника ставить работодателя в известность о таких изменениях в конкретный срок. Это избавит работодателя от многих проблем, например от неблагоприятных последствий, которые могут возникнуть при подаче в налоговый орган документов, содержащих недостоверные сведения о персональных данных работников.

Если у работника изменились, например, фамилия, имя, отчество или дата рождения, необходимо отразить это, в частности, в его трудовой книжке (если ведется).

При смене прописки изменения вносятся во все кадровые документы, где отражены данные о месте жительства (пребывания) работника.

Для внесения изменения в находящиеся у работодателя документы, которые содержат персональные данные соответствующего работника, рекомендуется составить в произвольной форме приказ.

См. образец составления приказа.

Внесение изменений в трудовой договор при изменении персональных данных (смена фамилии и т.д.)

Закон не обязывает работодателя вносить изменения в трудовой договор при изменении персональных данных работника. Однако рекомендуется все-таки отражать новые данные в договоре либо заключить дополнительное соглашение к нему, в котором отразить соответствующие изменения персональных данных работника.

Порядок изменения паспортных данных в трудовом договоре законодательно не установлен. Отметим, что согласно разъяснениям, размещенным на сайте "Онлайнинспекция.рф", работодателю следует заключить с работником дополнительное соглашение к трудовому договору, которым в договор будут внесены новые сведения (см. вопрос: Нужно ли менять паспортные данные в договоре при смене паспорта? Если да, то менять в каждом месте или достаточно это сделать единожды? Можно ли зачеркнуть ручкой и от руки написать? Прописать ли обоснование изменений? (сайт "Онлайнинспекция.рф", 2018) и вопрос: Нужно ли делать дополнительное соглашение к трудовому договору, если работник сменил паспорт? (сайт "Онлайнинспекция.рф", 2018)).

В дополнительном соглашении об изменении данных паспорта обычно указываются новые персональные данные работника, а также дата, с которой вносимые изменения вступают в силу.

Измениться могут и персональные данные работодателя - индивидуального предпринимателя. В этом случае стороны трудового договора также могут заключить допсоглашение к нему. Однако отсутствие такого соглашения не влечет прекращения или изменения трудовых отношений (Письмо Роструда от 04.06.2020 N ПГ/28836-6-1).

Передача персональных данных сотрудника

Условия передачи персональных данных работника третьим лицам

Работодатель вправе осуществлять передачу персональных данных работника третьим лицам, в том числе в коммерческих целях, только с его предварительного письменного согласия (абз. 2, 3 ч. 1 ст. 88 ТК РФ).

Работодатель может отказать в предоставлении персональных данных работника третьим

лицам, даже если работник дал письменное согласие. Исключение составляет случай, когда необходимость их предоставления установлена федеральными законами (ст. 7 Закона о персональных данных, абз. 2 ч. 1 ст. 88 ТК РФ).

Перед передачей персональных данных работодатель должен предупредить третье лицо о том, что они могут быть использованы только в тех целях, для которых были сообщены. При этом у третьего лица необходимо получить подтверждение того, что такое требование будет им соблюдено (абз. 4 ч. 1 ст. 88 ТК РФ).

Для защиты персональных данных от неправомерного использования работодатель обязан (абз. 5, 6, 7 ч. 1 ст. 88 ТК РФ):

а) осуществлять их передачу только в пределах одной организации;

б) регламентировать процедуру передачи персональных данных локальными нормативными актами (положение о персональных данных работников, утвержденный приказом список лиц, имеющих доступ к персональным данным, обязательство о неразглашении персональных данных);

в) ознакомить работников, которым открыт доступ к персональным данным других работников организации, с указанными локальными нормативными актами под подпись;

г) передавать персональные данные работников по мотивированному запросу только специально уполномоченным лицам, а также представителям работников в том объеме, который необходим им для выполнения конкретных функций.

Обязанность работодателя обеспечивать защиту персональных данных работника подтверждается судебной практикой. Так, суд указал, что работодатель правомерно не представил акционерам общества копию трудового договора с генеральным директором, поскольку ст. 88 ТК РФ установлен запрет на передачу персональных данных работника третьей стороне, а в соответствии со ст. 90 ТК РФ лица, виновные в нарушении норм, регулирующих защиту персональных данных, несут административную, гражданско-правовую или уголовную ответственность (см. Постановление ФАС Московского округа от 14.01.2010 N КА-А40/14463-09 по делу N А40-38438/09-17-269).

Ситуация из практики. **Может ли работодатель передавать персональные данные своих бывших работников новым работодателям по их запросам?**

Такие действия можно совершать только при наличии письменного согласия работника.

Из содержания п. 3 ст. 86 ТК РФ следует, что запрашивать информацию у третьей стороны, в том числе и у предыдущего работодателя, нынешний работодатель может только с согласия работника и только если данную информацию нельзя получить у самого работника. Иными словами, потенциальный работодатель вправе запросить информацию при наличии согласия работника, а прежний работодатель вправе ее передать с тем же условием.

В каких случаях не требуется согласие работника на передачу персональных данных?

NEW С 1 января 2023 г. вступают в силу изменения в Федеральный закон от 01.04.1996 N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования". См. Федеральный закон от 14.07.2022 N 237-ФЗ.

Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника (абз. 2 ст. 88 ТК РФ, абз. 1 п. 4 Разъяснений Роскомнадзора);
- в ФСС РФ, ПФР в объеме, предусмотренном законом (абз. 15 ч. 2 ст. 22 ТК РФ, п. 2 ст. 12 Федерального закона от 16.07.1999 N 165-ФЗ, ч. 2 ст. 15 Федерального закона от 01.04.1996 N 27-ФЗ, п. 2 ст. 14 Федерального закона от 15.12.2001 N 167-ФЗ, абз. 3 п. 4 Разъяснений Роскомнадзора);
- в налоговые органы (пп. 1, 2, 4 п. 3 ст. 24 НК РФ, п. 2 ст. 12 Закона об основах обязательного соцстрахования, абз. 5 п. 4 Разъяснений Роскомнадзора);
- в военные комиссариаты (абз. 4 п. 1 ст. 4 Федерального закона от 28.03.1998 N 53-ФЗ, пп. "г" п. 30, пп. "а" - "в", "д", "е" п. 32 Положения о воинском учете, утвержденного Постановлением Правительства РФ от 27.11.2006 N 719, абз. 5 п. 4 Разъяснений Роскомнадзора);
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства работодателем (абз. 5 ч. 6 ст. 370 ТК РФ, п. 1 ст. 17, п. 1 ст. 19 Федерального закона от 12.01.1996 N 10-ФЗ, абз. 5 п. 4 Разъяснений Роскомнадзора);
- по мотивированному запросу органов прокуратуры (п. 1 ст. 22 Федерального закона от 17.01.1992 N 2202-1, абз. 7 п. 4 Разъяснений Роскомнадзора);
- по мотивированному требованию правоохранительных органов и органов безопасности (ст. 6 Федерального закона от 29.07.2004 N 98-ФЗ, п. 4 ч. 1 ст. 13 Федерального закона от 07.02.2011 N 3-ФЗ, п. "м" ч. 1 ст. 13 Федерального закона от 03.04.1995 N 40-ФЗ, абз. 7 п. 4 Разъяснений Роскомнадзора);
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности (абз. 3 ч. 1 ст. 357 ТК РФ, абз. 7 п. 4 Разъяснений Роскомнадзора);
- по запросу суда. Это следует из анализа ч. 4 - 7 ст. 66 АПК РФ, ч. 1, 2 ст. 57 ГПК РФ;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом (абз. 5 ст. 228 ТК РФ). Перечень оповещаемых органов и сроки направления извещений о несчастном случае установлены ст. 228.1 ТК РФ;
- в случаях, связанных с исполнением работником должностных обязанностей (например, при направлении в командировку). Это следует из совокупного анализа ч. 5 - 5.2 ст. 11 Федерального закона от 09.02.2007 N 16-ФЗ, п. 13 Правил предоставления гостиничных услуг, утвержденных

Постановлением Правительства РФ от 18.11.2020 N 1853, абз. 4 п. 4 Разъяснений;

- для предоставления сведений в кредитную организацию, обслуживающую платежные карты работников, если в договоре о выпуске карт (коллективном договоре, локальном нормативном акте организации) предусмотрено право работодателя передавать персональные данные работников либо работодатель действует на основании доверенности на представление интересов работников (абз. 10 п. 4 Разъяснений).

Оформление согласия работника на передачу его персональных данных

В соответствии со ст. 88 ТК РФ передача персональных данных работника третьей стороне без письменного согласия указанного работника не разрешается, за исключением предусмотренных законом случаев. Также данной статьей предусмотрено, что без согласия работника персональные данные не могут передаваться в коммерческих целях. Соответственно, для передачи персональных данных необходимо письменное согласие работника. Из указанного документа должно быть понятно, кому будут передаваться персональные данные работника и с какой целью. Следует также учитывать, что в соответствии со ст. 88 ТК РФ работодатель обязан предупредить лиц, получающих персональные данные, о том, что данные сведения могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

Согласие на обработку персональных данных, разрешенных для распространения, нужно оформлять отдельно от иных согласий работника на обработку персональных данных. При этом ему необходимо дать возможность определить перечень персональных данных по каждой категории таких данных, указанной в согласии на их обработку. Молчание или бездействие работника нельзя считать согласием на обработку таких персональных данных (ч. 1, 8 ст. 10.1 Закона о персональных данных).

Указанное согласие работник предоставляет работодателю непосредственно либо с использованием информационной системы Роскомнадзора (ч. 6 ст. 10.1 Закона о персональных данных). На сайте ведомства действует сервис, который позволяет работодателю с учетом специфики своей деятельности сформировать шаблон формы согласия на обработку персональных данных, разрешенных для распространения. Шаблон рассмотрят специалисты Роскомнадзора и при необходимости дадут рекомендации по его доработке. В дальнейшем работодатель сможет использовать сформированную форму согласия в своей работе (Информация Роскомнадзора).

Правила использования информационной системы Роскомнадзора утверждены Приказом Роскомнадзора от 21.06.2021 N 106 в соответствии с ч. 7 ст. 10.1 Закона о персональных данных.

Требования к содержанию согласия на обработку персональных данных, разрешенных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 N 18.

Последствия передачи персональных данных работника без его согласия в случае, когда такое согласие обязательно

В соответствии со ст. 90 ТК РФ лица, которые виновны в нарушении норм, регулирующих обработку и защиту персональных данных работника, могут быть привлечены к дисциплинарной и материальной, а также к гражданско-правовой, административной и уголовной ответственности. Следовательно, передача персональных данных без согласия работника в случае, когда такое согласие обязательно, расценивается как нарушение законодательства о персональных данных. Работник может обратиться за защитой своих прав в государственные органы, к компетенции которых эти вопросы относятся. Необходимо иметь в виду, что за нарушение законодательства о персональных данных ответственность будут нести лицо, допустившее нарушение (единоличный исполнительный орган), и организация в целом.

Вопрос №3. Обязанности работодателя по защите персональных данных работников при их обработке и хранении

1. *Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных" {КонсультантПлюс}*
2. *Федеральный закон от 14.07.2022 N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" {КонсультантПлюс}*
3. *Федеральный закон от 28.05.2022 N 145-ФЗ "О внесении изменения в статью 14.8 Кодекса Российской Федерации об административных правонарушениях" {КонсультантПлюс}*
4. *Федеральный закон от 01.05.2022 N 135-ФЗ "О внесении изменения в статью 16 Закона Российской Федерации "О защите прав потребителей" {КонсультантПлюс}*
5. *Приказ Роскомнадзора от 05.08.2022 N 128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных" {КонсультантПлюс}*
6. *Указание Банка России от 16.12.2021 N 6017-У "О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой" {КонсультантПлюс}*
7. *ст. 13.11, "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 04.11.2022) {КонсультантПлюс}*
8. *ст. 14.57, "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 04.11.2022) {КонсультантПлюс}*

Содержание вопроса:

1. Какой комплект документов нужно создать для защиты персональных данных работников при обработке этих данных?
2. Как организовать защиту персональных данных работников при обработке этих данных, если они хранятся на бумажных носителях?
3. Как организовать защиту персональных данных работников при обработке этих данных, если они хранятся в электронном виде?
4. Что делать, если персональные данные работников неправомерно или случайно переданы (предоставлены, распространены и т.д.)?

Работодатель обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных работников от неправомерного использования или утраты либо

обеспечить принятие таких мер. Это следует из п. 7 ст. 86 ТК РФ, ч. 1 ст. 19 Закона о персональных данных.

В частности, работодатель может предусмотреть в локальном нормативном акте требования к помещениям, в которых находятся носители информации (например, компьютеры с базами данных, документы на бумажных носителях), содержащие персональные данные работников.

Обращаем внимание, что Закон о персональных данных и Трудовой кодекс РФ не устанавливают каких-либо требований к упомянутым помещениям. Представляется, что работодатель может определить особый режим доступа в них, требования к оборудованию, установить перечень лиц, имеющих право доступа в данные помещения. Такие выводы следуют из анализа ч. 1, 2 ст. 19 Закона о персональных данных, ч. 1 ст. 8, абз. 7 ч. 1 ст. 22, ст. 87 ТК РФ.

Исходя из п. 21 Методических рекомендаций по ведению воинского учета в организациях (утв. Минобороны России 11.07.2017) документы воинского учета, содержащие персональные данные работников, рекомендуем хранить в железных шкафах в специально оборудованных помещениях.

Какой комплект документов нужно создать для защиты персональных данных работников при обработке этих данных?

Для защиты персональных данных работников создайте комплект следующих основных документов:

1) приказ о назначении лица, ответственного за организацию обработки персональных данных работников (п. 1 ч. 1 ст. 18.1 Закона о персональных данных).

Ответственного за обработку персональных данных назначьте приказом. Им может быть любой работник вашей организации, например специалист отдела по управлению персоналом. Главное, чтобы он смог выполнять обязанности, перечисленные в ч. 4 ст. 22.1 Закона о персональных данных.

Например, он должен доводить до сведения работников положения законодательства о персональных данных, а также ваших локальных актов об обработке персональных данных (п. 2 ч. 4 ст. 22.1 Закона о персональных данных).

Если вы поручили обработку персональных данных другому лицу по договору с ним, учтите требования, перечисленные в ч. 3 ст. 6 Закона о персональных данных;

2) положение о защите персональных данных работников или иной локальный нормативный акт, регулирующий порядок хранения, использования, обработки таких данных. Учтите требования и ограничения к содержанию такого документа. В нем не должно быть положений, ограничивающих права работников, а также возлагающих на вас полномочия и обязанности, не предусмотренные законом (ст. 87 ТК РФ, п. 2 ч. 1 ст. 18.1 Закона о персональных данных);

3) приказ об утверждении перечня лиц, имеющих доступ к персональным данным работников. Такой приказ следует издать во исполнение требований абз. 6 ст. 88 ТК РФ.

Рекомендуем у всех этих лиц взять письменное обязательство о неразглашении (соблюдении

конфиденциальности) персональных данных, учитывая абз. 4 ст. 88 ТК РФ, ч. 3 ст. 6 Закона о персональных данных.

Вы можете включить в этот комплект и другие необходимые для вас документы. Например, это могут быть журналы учета персональных данных, их выдачи и передачи другим лицам, представителям сторонних организаций и государственным органам.

Если речь идет о защите информации ограниченного доступа, не составляющей гостайну, объекты информатизации (например, государственные информационные системы персональных данных) подлежат аттестации на соответствие требованиям по защите такой информации. Состав и содержание работ по аттестации, а также требования к форме и содержанию разрабатываемых при организации и проведении таких работ документов определены Порядком, утвержденным Приказом ФСТЭК России от 29.04.2021 N 77.

Как организовать защиту персональных данных работников при обработке этих данных, если они хранятся на бумажных носителях?

Требования к организации защиты персональных данных на бумажных носителях подробно не описаны в законе. Ключевое требование закона - вы должны принимать необходимые правовые, организационные и технические меры для защиты персональных данных работников от неправомерного использования или утраты либо обеспечить принятие таких мер (п. 7 ст. 86 ТК РФ, ч. 1 ст. 19 Закона о персональных данных).

Поэтому мы рекомендуем, в частности, следующее:

1) хранить персональные данные на бумажных носителях в специальных помещениях. Учитывайте, что нужно раздельно хранить персональные данные (материальные носители), которые обрабатываются в разных целях (п. 14 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации);

2) организовать особый режим доступа в эти помещения, в частности утвердить перечень лиц, имеющих доступ в данные помещения с учетом требований п. 13 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации;

3) организовать охрану таких помещений, например оборудовать их сигнализацией, металлическими самозакрывающимися дверьми, решетками на окнах.

Обратите внимание, что в некоторых случаях обязательно хранить персональные данные в железных шкафах. Например, в таких шкафах должны храниться документы воинского учета, содержащие персональные данные работников (п. 21 Методических рекомендаций по ведению воинского учета в организациях).

Как организовать защиту персональных данных работников при обработке этих данных, если они хранятся в электронном виде?

Организовать защиту персональных данных, которые хранятся в информационных системах, непросто. Основное требование закона - вы должны принимать необходимые правовые, организационные и технические меры для защиты персональных данных работников от неправомерного использования или утраты либо обеспечить принятие таких мер (п. 7 ст. 86 ТК РФ, ч. 1 ст. 19 Закона о персональных данных).

Но есть множество уточнений, с которыми сложно разобраться неспециалисту. Вы можете удостовериться в этом, изучив организационные и технические меры, которые утверждены Приказом ФСТЭК России от 18.02.2013 N 21 и Приказом ФСБ России от 10.07.2014 N 378.

Поэтому, как правило, привлекают специализированную организацию или ИП, у которых есть лицензия на деятельность по технической защите конфиденциальной информации (п. 2 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных).

В частности, для защиты персональных данных потребуется:

1) определить, какой у вас тип угрозы безопасности персональных данных (п. 7 Требований к защите персональных данных при их обработке в информационных системах);

2) подобрать один из четырех уровней защищенности персональных данных, исходя из вашего типа угрозы, в соответствии с п. п. 8 - 16 Требований к защите персональных данных при их обработке в информационных системах.

Именно от этого и будет зависеть комплекс мер.

Например, если по итогам определения типа угрозы специалист предложит вам обеспечить минимальный (четвертый) уровень защищенности персональных данных работников, вам потребуется (п. 13 Требований к защите персональных данных при их обработке в информационных системах):

- обезопасить помещения, в которых размещена информационная система, от неконтролируемого проникновения или неправомерного доступа;
- обеспечить сохранность носителей персональных данных;
- утвердить перечень лиц, имеющих в силу трудовых обязанностей доступ к персональным данным в информационной системе;
- защитить информацию с помощью средств, прошедших процедуру оценки соответствия (в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз).

Кроме того, вы обязаны взаимодействовать с госсистемой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. В частности, потребуется уведомлять о компьютерных инцидентах, из-за которых персональные данные неправомерно переданы (предоставлены, распространены и т.д.) (ч. 12 ст. 19 Закона о персональных данных).

Что делать, если персональные данные работников неправомерно или случайно переданы (предоставлены, распространены и т.д.)?

Если передача данных привела к нарушению прав работников, вы обязаны в течение 24 часов с момента ее выявления уведомить Роскомнадзор (п. 1 ч. 3.1 ст. 21 Закона о персональных данных):

- об инциденте и его предполагаемых причинах;
- возможном вреде, причиненном правам работников;
- принятых мерах по устранению последствий инцидента;
- лице, которое вы уполномочили взаимодействовать с Роскомнадзором по вопросам, связанным с инцидентом.

По выявленному факту вы обязаны провести внутреннее расследование. О его результатах нужно уведомить Роскомнадзор в течение 72 часов с момента обнаружения передачи данных. Кроме того, надо предоставить сведения о лицах, из-за которых произошел инцидент (если такие есть) (п. 2 ч. 3.1 ст. 21 Закона о персональных данных).

Формы уведомлений размещены на сайте Роскомнадзора (Информация Роскомнадзора).

Рекомендации:

1. разработайте локальную процедуру выявления, установления, нейтрализации и уведомления в отношении инцидентов неправомерного раскрытия ПД. Особый фокус следует уделить выявлению и мониторингу инцидентов в СМИ, интернет-ресурсах и иных открытых источниках. Также можно организовать программу по «охоте» за такого рода сведениями с привлечением всех заинтересованных лиц («Data Breach Bounty») путем выплаты вознаграждения за предоставление сведений о таких инцидентах;

2. проверьте, соответствуют ли типовые формы договоров об обработке ПД новым требованиям в отношении инцидентов неправомерного раскрытия персональных данных. Внесите изменения в уже заключенные договоры.

Вопрос №4. Порядок организации работ по обеспечению безопасности персональных данных работников при обработке и хранении

1. *Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных" {КонсультантПлюс}*
2. *Федеральный закон от 14.07.2022 N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" {КонсультантПлюс}*
3. *Федеральный закон от 28.05.2022 N 145-ФЗ "О внесении изменения в статью 14.8 Кодекса Российской Федерации об административных правонарушениях" {КонсультантПлюс}*
4. *Федеральный закон от 01.05.2022 N 135-ФЗ "О внесении изменения в статью 16 Закона Российской Федерации "О защите прав потребителей" {КонсультантПлюс}*
5. *Приказ Роскомнадзора от 05.08.2022 N 128 "Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных" {КонсультантПлюс}*
6. *Указание Банка России от 16.12.2021 N 6017-У "О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой" {КонсультантПлюс}*
7. *ст. 13.11, "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 04.11.2022) {КонсультантПлюс}*
8. *ст. 14.57, "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 04.11.2022) {КонсультантПлюс}*

Содержание вопроса:

1. Организация доступа работников к персональным данным других работников
2. Оформление обязательства о неразглашении персональных данных работниками, имеющими доступ к этим данным
3. Как составить и утвердить положение об обработке и защите персональных данных?
4. Оформление Положения об обработке и защите персональных данных

Защита персональных данных представляет собой регламентированный технологический процесс, предупреждающий нарушение установленного порядка доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий безопасность информации в процессе управленческой и производственной деятельности компании.

Для обеспечения внешней защиты персональных данных работников работодатель должен принять следующие меры:

- установить пропускной режим и особый порядок приема, учета и контроля деятельности посетителей;
- установить особый порядок выдачи пропусков и удостоверений работников;
- использовать технические средства охраны;
- использовать программно-технический комплекс защиты информации на электронных носителях и пр.

Для обеспечения внутренней защиты персональных данных работников работодатель должен предпринять следующее:

- ограничить и регламентировать состав работников, функциональные обязанности которых требуют доступа к персональным данным других работников;
- избирательно и обоснованно распределить документы и информацию, содержащую персональные данные, между лицами, уполномоченными на работу с такими данными;
- рационально размещать рабочие места для исключения бесконтрольного использования защищаемой информации;
- регулярно проверять знание работниками, имеющими отношение к работе с персональными данными, требований нормативно-методических документов по защите таких данных;
- создавать необходимые условия для работы с документами и базами данных, содержащими персональные данные работников;
- определять состав работников, имеющих право доступа (входа) в помещения, в которых хранятся персональные данные;
- организовать порядок уничтожения информации;
- своевременно выявлять и устранять нарушения установленных требований по защите персональных данных работников;
- проводить профилактическую работу с должностными лицами, имеющими доступ к персональным данным работников, по предупреждению разглашения таких сведений.

Организация доступа работников к персональным данным других работников

В соответствии со ст. 88 ТК РФ работодатель обязан не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью последнего, а также в других случаях, предусмотренных Трудовым кодексом РФ или иными федеральными законами.

Однако возникают случаи, когда отдельным работникам нужно получить информацию о персональных данных других работников, которые они намереваются использовать при выполнении трудовых обязанностей. Например, бухгалтеру могут понадобиться данные о работнике для начисления ему заработной платы или уплаты соответствующих взносов, при направлении работников в командировку секретарю (или иному лицу) понадобятся паспортные данные последних для покупки билетов, юрисконсульту организации данные работников могут

понадобиться для оформления доверенностей и т.д. В соответствии со ст. 88 ТК РФ работодатель может разрешить доступ к персональным данным работников только специально уполномоченным лицам, при этом указанным лицам будут доступны только те данные, которые необходимы для выполнения конкретных функций. Например, доступ к персональным данным работников обычно устанавливается для руководителя организации, руководителей структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения), руководителю нового подразделения - при переводе сотрудника из одного структурного подразделения в другое, работникам бухгалтерии и отдела кадров. Конкретный перечень работников, которые имеют доступ к персональным данным других работников, должен быть установлен локальным нормативным актом организации и приказом организации. Подробнее об этом см. п. 4 настоящего материала.

См. образец составления приказа.

Оформление обязательства о неразглашении персональных данных работниками, имеющими доступ к этим данным

В соответствии с п. 7 ст. 86 ТК РФ на работодателя возложена обязанность по защите персональных данных работника от неправомерного их использования или утраты. Следовательно, работники, которые имеют доступ к персональным данным других работников, обязаны не разглашать эти данные, которые стали им известны в связи с выполнением ими трудовых обязанностей. При этом привлечь к ответственности работников, которые разгласили такую информацию, можно, только если она стала известна им в связи с исполнением трудовых обязанностей и они обязались не разглашать такие сведения (п. 43 Постановления Пленума Верховного Суда РФ от 17.03.2004 N 2). Следовательно, работодатель должен оформить с работниками, которые в силу своих должностных обязанностей имеют доступ к персональным данным других работников, обязательство об их неразглашении.

Как составить и утвердить положение об обработке и защите персональных данных?

В соответствии со ст. 87 ТК РФ порядок хранения и использования персональных данных работников устанавливается работодателем с учетом требований Трудового кодекса РФ и иных федеральных законов. Данная норма обязывает работодателя принять локальный акт, который будет регулировать порядок хранения и использования персональных данных. Таким актом обычно является Положение об обработке и защите персональных данных. Согласно п. 8 ст. 86 ТК РФ работники и их представители должны быть ознакомлены под подпись с документами, устанавливающими порядок обработки и защиты персональных данных, а также их права и обязанности в этой области.

Ситуация из практики. **Является ли локальный нормативный акт, например положение об обработке и защите персональных данных, обязательным документом?**

В организации должен быть локальный нормативный акт (несколько ЛНА) по вопросам обработки персональных данных, включая установление процедур, направленных на предотвращение и выявление нарушений законодательства в области персональных данных (п. 2 ч. 1 ст. 18.1 Закона о персональных данных).

Порядок хранения и использования персональных данных работников устанавливает работодатель с соблюдением требований федеральных законов (ст. 87 ТК РФ).

Таким ЛНА может быть, например, положение об обработке и защите персональных данных.

Оформление Положения об обработке и защите персональных данных

Положение можно разработать в произвольной форме, так как нормативной нет. С документом нужно ознакомить под подпись тех работников, с чьей трудовой деятельностью он непосредственно связан. Это касается, например, лиц, которые непосредственно обрабатывают персональные данные (ч. 2 ст. 22 ТК РФ, п. 6 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ).

Структура Положения с учетом требований п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ может быть следующей:

1) "Общие положения" - отражаются вопросы, которые регулирует Положение, порядок его вступления в силу, внесения изменений;

2) "Категории субъектов персональных данных" - указываются физлица (например, работники, соискатели), персональные данные которых будут обрабатываться согласно Положению;

3) "Цели обработки персональных данных, категории и перечни обрабатываемых персональных данных" - перечисляются цели обработки и данные, которые будут обрабатываться для их достижения;

4) "Порядок и условия обработки персональных данных" - регулируются, например, способы обработки таких данных;

5) "Сроки обработки и хранения персональных данных" - указывается, в частности, сколько нужно хранить документы, которые содержат персональные данные;

6) "Порядок блокирования и уничтожения персональных данных" - определяются, например, сроки уничтожения персональных данных при достижении максимальных сроков хранения документов, в которых они содержатся;

7) "Защита персональных данных. Процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений" - перечисляются локальные нормативные акты, которые принимаются во исполнение Положения, указывается

порядок осуществления контроля за соблюдением у работодателя требований законодательства в области персональных данных и т.п.;

8) "Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных" - указываются последствия нарушения законодательства в области персональных данных.

См. образец составления Положения.

Введение в действие Положения об обработке и защите персональных данных

Положение об обработке и защите персональных данных, как и любой другой локальный нормативный акт, издается и утверждается работодателем путем издания приказа, который подписывает руководитель организации или иное уполномоченное на это лицо. При наличии в организации представительного органа работников названное Положение должно приниматься с учетом требований ст. 372 ТК РФ. Согласно данной статье перед принятием решения об издании локального нормативного акта работодатель направляет его проект и обоснование его издания в выборный орган первичной профсоюзной организации, представляющий интересы всех или большинства работников. Данный орган не позднее пяти рабочих дней со дня получения проекта указанного локального нормативного акта направляет работодателю мотивированное мнение о проекте, составленное в письменной форме. В случае если это мнение выражает несогласие с проектом либо содержит предложения по его совершенствованию, работодатель может согласиться с мнением профсоюзного органа либо в течение трех дней после его получения провести дополнительные консультации с указанным органом в целях достижения решения, устраивающего обе стороны. Если согласие не достигнуто, возникшие разногласия оформляются протоколом, после чего работодатель имеет право своим решением принять локальный нормативный акт. В свою очередь профсоюзный орган может обжаловать это решение в соответствующую государственную инспекцию труда или в суд. Также согласно ч. 4 ст. 372 ТК РФ указанный орган может начать коллективный трудовой спор в соответствии с нормами Трудового кодекса РФ.

Ознакомление с Положением об обработке и защите персональных данных работников (иных лиц)

Исходя из требований ст. ст. 68, 86 ТК РФ работники и их представители должны быть под подпись ознакомлены с Положением об обработке и защите персональных данных работников (иных лиц). Факт ознакомления с указанным Положением может фиксироваться как в тексте самого трудового договора (путем перечисления локальных нормативных актов, с которыми работник ознакомлен до подписания договора), так и в отдельном документе (в самом Положении на листе ознакомления с ним). Работодатель может также предусмотреть в организации журнал ознакомления работников с локальными нормативными актами, где работники будут расписываться в подтверждение того, что они ознакомлены с соответствующими актами (в том

числе с Положением об обработке и защите персональных данных работников (иных лиц)).

Вопрос №5. Ответственность за нарушение норм законодательства о персональных данных

1. *Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных" {КонсультантПлюс}*
2. *Указание Банка России от 16.12.2021 N 6017-У "О перечне угроз безопасности, актуальных при обработке биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, при взаимодействии организаций финансового рынка с единой биометрической системой" {КонсультантПлюс}*
3. *ст. 13.11, "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 04.11.2022) {КонсультантПлюс}*
4. *ст. 14.57, "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 04.11.2022) {КонсультантПлюс}*

Содержание вопроса:

1. Какая административная ответственность грозит за нарушение законодательства о персональных данных?
2. В чем состоит гражданско-правовая ответственность?
3. Какую ответственность несут работник и работодатель за нарушения законодательства о персональных данных?
4. В каких случаях нарушение законодательства о защите персональных данных может повлечь уголовную ответственность?

Если Вы обрабатываете персональные данные граждан (например, клиентов, сотрудников), то за нарушения по работе с этими данными вас могут привлечь прежде всего к административной ответственности. Например, административный штраф может быть назначен за сбор персональных данных в ненадлежащих целях.

Гражданско-правовая ответственность наступит, если вы причинили убытки или моральный вред гражданину. Своих сотрудников, допустивших нарушение, вы можете привлечь к дисциплинарной и материальной ответственности. Как работодатель вы отвечаете за нарушение правил работы с персональными данными работников.

Если действия физлица содержат признаки преступления, то его могут привлечь к уголовной ответственности.

Какая административная ответственность грозит за нарушение законодательства о персональных данных?

Административная ответственность установлена:

- за нарушение правил обработки персональных данных;
- неисполнение обязанностей при взаимодействии с гражданином - субъектом персональных данных;
- невыполнение требований по защите персональных данных;
- неисполнение обязанностей при взаимодействии с Роскомнадзором.

Если в ходе проверки будет выявлено два и более нарушения, ответственность за которые предусмотрена одной и той же статьей (частью статьи) разд. II КоАП РФ, вас накажут как за одно. Если же ответственность за выявленные нарушения предусмотрена двумя и более статьями (их частями), грозить будет одно - наиболее строгое - наказание. В последнем случае могут назначить и дополнительные санкции (ч. 2 - 6 ст. 4.4 КоАП РФ).

Обратите внимание, что к ответственности за нарушение могут одновременно привлечь и организацию, и виновное физическое лицо, за исключением ряда случаев. Например, юрлицо не привлекут к ответственности, если привлекли его должностное лицо (работника). Избежать наказания сможет то юрлицо, которое приняло все предусмотренные законодательством меры для соблюдения соответствующих правил и норм (ч. 3 - 4 ст. 2.1 КоАП РФ).

Основной вид административного наказания за нарушение законодательства о персональных данных - штраф. Его размер зависит от конкретного нарушения. Например, максимальный штраф для организации за обработку персональных данных без письменного согласия гражданина, когда согласие требуется, или за отсутствие в нем всех необходимых сведений составляет 150 000 руб., за повторное правонарушение - 500 000 руб. (ч. 2, 2.1 ст. 13.11 КоАП РФ).

Далее рассмотрим подробнее группы нарушений и размеры штрафов за них.

Когда вместо административного штрафа возможно предупреждение

Это возможно, если наказание в виде предупреждения не предусмотрено за ваше нарушение, оно выявлено в ходе государственного контроля (надзора), муниципального контроля, вы совершили его впервые и при этом соблюдены условия, перечисленные в ч. 2 ст. 3.4 КоАП РФ. Однако при совершении некоторых нарушений штраф заменить нельзя (ч. 3 ст. 3.4, ч. 2 ст. 4.1.1 КоАП РФ).

Каковы особенности назначения административного штрафа СОНКО и малым предприятиям (включая микропредприятия), относящимся к СМСП

В определенных случаях таким организациям административный штраф может назначаться с учетом размеров штрафов для ИП и должностных лиц (ч. 1 - 3 ст. 4.1.2 КоАП РФ).

Например, если организация является малым предприятием и на момент совершения

правонарушения включена в соответствующий реестр, то штраф назначат в размере, предусмотренном для ИП. При этом если санкцией статьи не предусмотрен штраф для ИП, то он назначается в размере от половины минимального до половины максимального размера штрафа, предусмотренного для юрлица, или в размере половины фиксированного штрафа для юрлица. Размер штрафа, назначаемого по ч. 2 ст. 4.1.2 КоАП РФ, не может быть меньше минимального размера соответствующего штрафа для должностного лица (ч. 1, 2, 3 ст. 4.1.2 КоАП РФ).

Для СОНКО при привлечении к ответственности по ч. 2 ст. 13.11 КоАП РФ размер штрафа будет составлять от 15 тыс. до 75 тыс. руб.

Необходимо учитывать, что правило о снижении штрафов не действует, если нормой о правонарушении ИП в части ответственности приравнены к юрлицам (ч. 4 ст. 4.1.2 КоАП РФ).

Административная ответственность за нарушение правил обработки персональных данных

К административной ответственности за нарушение правил обработки вашу организацию и ее должностных лиц могут привлечь, если вы будете обрабатывать персональные данные:

1) **в не предусмотренных законом случаях** (ч. 1 ст. 13.11 КоАП РФ).

Максимальный штраф для должностных лиц - 20 000 руб., для организации - 100 000 руб.

Перечень случаев, в которых допускается обработка персональных данных, установлен в ч. 1 ст. 6 Закона о персональных данных. К их числу относится и обработка с согласия физлица, но обратите внимание, что под него состав отдельный - по ч. 2 ст. 13.11 КоАП РФ;

2) **в целях, несовместимых с целями сбора** (ч. 1 ст. 13.11 КоАП РФ).

Максимальный штраф для должностных лиц - 20 000 руб., для организации - 100 000 руб.

Учтите, что у вас должны быть заранее определены законные и конкретные цели обработки персональных данных и все ваши действия с персональными данными должны им соответствовать (ч. 2, 5 ст. 5 Закона о персональных данных).

За повторное нарушение правил обработки персональных данных максимальный штраф составит: для должностных лиц - 50 000 руб., для ИП - 100 000 руб., для организации - 300 000 руб. (ч. 1.1 ст. 13.11 КоАП РФ);

3) **без согласия**, когда оно требуется, или с согласия, но с неполными сведениями (ч. 2 ст. 13.11 КоАП РФ).

Максимальный штраф для должностных лиц - 40 000 руб., для организации - 150 000 руб.

За повторное нарушение максимальный штраф составит: для должностных лиц - 100 000 руб., для ИП - 300 000 руб., для организации - 500 000 руб. (ч. 2.1 ст. 13.11 КоАП РФ).

Обратите внимание, что согласие требуется далеко не всегда, есть большой перечень случаев, когда в нем нет необходимости;

4) **без использования баз данных, находящихся в России**, для записи, систематизации, накопления, хранения, уточнения (обновления, изменения) или извлечения персональных данных граждан РФ (ч. 5 ст. 18 Закона о персональных данных, ч. 8, 9 ст. 13.11 КоАП РФ).

Максимальный штраф за неисполнение этой обязанности для должностных лиц - 200 000 руб. (за повторное нарушение - 800 000 руб.), для организации либо индивидуального предпринимателя - 6 000 000 руб. (за повторное нарушение - 18 000 000 руб.).

Административная ответственность за неисполнение оператором обязанностей при взаимодействии с гражданином

Вас могут привлечь к ответственности, если вы:

1) в определенный срок **не представите гражданину запрошенную им информацию** (ч. 4 ст. 13.11 КоАП РФ).

Максимальный штраф для должностных лиц - 12 000 руб., для организации - 80 000 руб., для ИП - 30 000 руб.

Вас могут привлечь к ответственности, если вы, например, не подтвердите, что вы обрабатываете персональные данные, в течение 10 рабочих дней (если этот срок не был продлен) с получения соответствующего запроса гражданина (его представителя) (ч. 7 ст. 14, ч. 1 ст. 20 Закона о персональных данных);

2) **не выполните требование об уточнении, блокировании или уничтожении** его персональных данных, если они неполные, неточные, устарели, были незаконно получены или не являются необходимыми для целей обработки (ч. 5, 5.1 ст. 13.11 КоАП РФ).

Максимальный штраф для должностных лиц - 20 000 руб. (за повторное нарушение - 50 000 руб.), для организации - 90 000 руб. (за повторное нарушение - 500 000 руб.), для ИП - 40 000 руб. (за повторное нарушение - 100 000 руб.).

В частности, к ответственности вас могут привлечь, если вы не уточните персональные данные в течение семи рабочих дней со дня представления субъектом актуальных сведений (ч. 2 ст. 21 Закона о персональных данных).

Административная ответственность за невыполнение требований по защите персональных данных

К такой ответственности вас могут привлечь, если вы:

1) **не опубликуете необходимые документы** о вашей политике в отношении обработки персональных данных и о том, какие требования по их защите вы реализуете, или не обеспечите иным образом неограниченный доступ к ним (ч. 3 ст. 13.11 КоАП РФ).

Максимальный штраф для должностных лиц - 12 000 руб., для организации - 60 000 руб., для ИП - 20 000 руб.;

2) **не обеспечите сохранность данных** при их неавтоматизированной обработке, если это

повлечет неправомерный или случайный доступ к ним, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия (ч. 6 ст. 13.11 КоАП РФ).

Максимальный штраф для должностных лиц - 20 000 руб., для организации - 100 000 руб., для ИП - 40 000 руб.

Административная ответственность за неисполнение оператором обязанностей при взаимодействии с Роскомнадзором

К административной ответственности при взаимодействии с Роскомнадзором - уполномоченным органом по защите прав субъектов персональных данных вас могут привлечь, если вы, в частности:

не представите информацию, запрошенную им в порядке ч. 3 ст. 23 Закона о персональных данных (ст. 19.7 КоАП РФ);

- не выполните в срок законное предписание Роскомнадзора об устранении нарушений (ч. 1 ст. 19.5 КоАП РФ);
- будете препятствовать проведению проверки либо уклоняться от нее (ч. 1 ст. 19.4.1 КоАП РФ);
- не выполните требование Роскомнадзора об уточнении, блокировании или уничтожении персональных данных, если они неполные, неточные, устарели, были незаконно получены или не являются необходимыми для целей обработки (ч. 5 ст. 13.11 КоАП РФ).

В чем состоит гражданско-правовая ответственность?

Нарушение законодательства в области персональных данных может повлечь гражданско-правовую ответственность в форме компенсации морального вреда, возмещения убытков, взыскания неустойки, если она была предусмотрена вашим договором.

Обратите внимание, что моральный вред вы обязаны возместить вне зависимости от того, возмещали ли вы имущественный вред физлицу и понесенные им убытки (ч. 2 ст. 24 Закона о персональных данных).

Ваша ответственность может наступить, если вы нарушаете:

- права субъекта, установленные Законом о персональных данных;
- правила обработки персональных данных;
- требования к их защите.

Компенсировать моральный вред вы будете в денежной форме, размер компенсации определит суд с учетом степени вашей вины и степени страданий гражданина (ст. ст. 151, 1101 ГК РФ).

Убытки суд взыщет, если будут доказаны наступление вреда, противоправность вашего поведения и ваша вина, а также причинно-следственная связь между ними (см. Позицию КС РФ, ВС РФ,

ВАС РФ). Учтите, что вина презюмируется и ее отсутствие придется доказывать вам (п. 2 ст. 1064 ГК РФ).

Обратите внимание, что возмещать вред будет организация, а не должностные лица, поскольку вред, причиненный работником, должен возмещать работодатель (п. 1 ст. 1068 ГК РФ).

Какую ответственность несут работник и работодатель за нарушения законодательства о персональных данных?

Работодатель в этом случае может понести материальную ответственность перед своими сотрудниками.

Работника можно привлечь как к дисциплинарной, так и к материальной ответственности, если по его вине при обработке персональных данных произошло нарушение законодательства в области персональных данных.

Какую ответственность несет работодатель перед своими работниками?

Вы несете материальную ответственность перед своими работниками, если, нарушив по своей вине законодательство в области персональных данных, причините им материальный ущерб и (или) моральный вред (ст. 90, ч. 1 ст. 232, ч. 1 ст. 233 ТК РФ).

Например, такое возможно, если вы не обеспечили защиту персональных данных работника (не организовали особый режим доступа, хранение в особых местах и так далее), из-за чего они стали доступны посторонним лицам.

В таком случае вы обязаны возместить работнику ущерб в полном объеме, а моральный вред - в той сумме, о которой договоритесь с работником или которую определит суд (ч. 1 ст. 235, ст. 237 ТК РФ).

Дисциплинарная ответственность для работодателя законодательством не предусмотрена.

К какой ответственности работодатель может привлечь работника?

Вы можете привлечь работника к дисциплинарной и материальной ответственности, если он по своей вине нарушил нормы, регулирующие обработку и защиту персональных данных других работников. Но потребуется соблюсти определенные условия (ч. 1 ст. 22, ст. 90 ТК РФ).

Дисциплинарная ответственность работника

Работника можно привлечь к дисциплинарной ответственности, если он виноват в неисполнении (ненадлежащем исполнении) своих трудовых обязанностей по обработке персональных данных (ч. 1 ст. 192 ТК РФ). Например, такое возможно, если работник отдела кадров разгласит персональные данные других лиц, которые стали ему известны в связи с исполнением своих трудовых обязанностей и которые он обязался не разглашать.

Такие действия могут быть признаны однократным грубым нарушением работником трудовых обязанностей. И в этом случае вы вправе применить к нему дисциплинарное взыскание вплоть до увольнения по пп. "в" п. 6 ч. 1 ст. 81 ТК РФ.

Учтите только, что нельзя уволить по этому основанию беременную женщину, работника, который находится в отпуске или на больничном, а также несовершеннолетнего, если нет на это согласия трудинспекции и комиссии по делам несовершеннолетних и защите их прав (пп. "в" п. 6 ч. 1, ч. 6 ст. 81, ч. 1 ст. 261, ст. 269 ТК РФ).

Чтобы привлечь работника к дисциплинарной ответственности, в том числе в виде увольнения, вам потребуется соблюсти специальный порядок, в частности: затребовать у него письменное объяснение, составить акт, если работник не представит его по истечении двух рабочих дней, оформить приказ о наложении дисциплинарного взыскания и ознакомить с ним работника (ч. 1, 2 ст. 192, ч. 1, 6 ст. 193 ТК РФ).

Материальная ответственность работника

Вы можете привлечь работника, ответственного за обработку персональных данных, в том числе за их неразглашение, если он нарушил свои обязанности и причинил вам тем самым ущерб (ст. 90, ч. 1 ст. 238 ТК РФ). То есть если вам пришлось возмещать материальный ущерб и (или) моральный вред пострадавшим по его вине работникам или третьим лицам.

Взыскать можно только прямой действительный ущерб, в том числе сумму ущерба и (или) морального вреда, выплаченную вами пострадавшим по его вине работникам или третьим лицам (ст. 90, ч. 1 ст. 238 ТК РФ).

Но сначала обязательно проведите проверку для определения размера ущерба и причин его возникновения, истребуйте от работника письменное объяснение, а также учтите другие обязательные требования, предусмотренные ст. ст. 246, 247, 248 ТК РФ.

В каких случаях нарушение законодательства о защите персональных данных может повлечь уголовную ответственность?

Специальной нормы об ответственности за нарушение Закона о персональных данных в Уголовном кодексе РФ нет. Однако действия лица, нарушившего правила работы с персональными данными, могут образовать состав преступления из числа предусмотренных Уголовным кодексом РФ.

В частности, уголовная ответственность установлена:

- за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную и семейную тайну, без его согласия (ч. 1 ст. 137 УК РФ);
- неправомерный доступ к компьютерной информации, в результате которого произошло уничтожение, блокирование, модификация (изменение) или копирование информации (ч. 1 ст. 272

УК РФ);

- неправомерный отказ должностного лица в представлении гражданину документов и материалов, собранных в установленном порядке и непосредственно затрагивающих его права и свободы гражданина (ст. 140 УК РФ).

Учтите, что к уголовной ответственности могут привлечь только физическое лицо (ст. 19 УК РФ). Однако привлечение виновного физического лица к уголовной ответственности не освобождает от административной ответственности организацию (ч. 3 ст. 2.1 КоАП РФ).

Таблица – Какие штрафы грозят за нарушение норм законодательства о персональных данных?

Нарушение	Наказание	Норма КоАП РФ
Обработка персональных данных не предусмотрена законом или несовместима с целями сбора данных (например, в положении указаны одни цели для сбора данных, а их собирают и для других, допустим, для маркетинговых целей)	Штраф: - для должностных лиц – от 10 000 до 20 000 рублей; - для юрлица – от 60 000 до 100 000 рублей.	Ч. 1 ст. 13.11
Нет согласия субъекта или есть другие нарушения обработки персональных данных (например, компания неправильно хранит данные субъекта при их обработке на бумаге, бумажный носитель не убирают в шкаф (сейф))	Штраф: - для должностных лиц – от 20 000 до 40 000 рублей; - для юрлица – от 30 000 до 150 000 рублей.	Ч. 2 ст. 13.11
Оператор не предоставил доступ к политике по обработке персональных данных (например, не опубликовал на сайте)	Штраф: - для должностных лиц – от 6 000 до 12 000 рублей; - для ИП – от 10 000 до 20 000 рублей; - для юрлица – от 30 000 до	Ч. 3 ст. 13.11

	60 000 рублей.	
Оператор не предоставляет субъекту персональных данных информацию, которая касается обработки его ПД	Штраф: - для должностных лиц – от 8 000 до 12 000 рублей; - для ИП – от 20 000 до 30 000 рублей; - для юрлица – от 40 000 до 80 000 рублей.	Ч. 4 ст. 13.11
Оператор не выполняет в срок требования субъекта персональных данных, его представителя либо Роскомнадзора об уточнении ПД, их блокировании или уничтожении	Штраф: - для должностных лиц – от 8 000 до 20 000 рублей; - для ИП – от 20 000 до 40 000 рублей; - для юрлица – от 50 000 до 90 000 рублей.	Ч. 5 ст. 13.11
Оператор не выполнил при обработке ПД на бумажных носителях обязанности по соблюдению условий, обеспечивающих их сохранность и исключающих незаконный к ним доступ, если это повлекло доступ к данным	Штраф: - для должностных лиц – от 8 000 до 20 000 рублей; - для ИП – от 20 000 до 40 000 рублей; - для юрлица – от 50 000 до 100 000 рублей.	Ч. 6 ст. 13.11
Оператор обрабатывает персональные данные с использованием баз данных, находящихся за пределами территории РФ	Штраф: - для должностных лиц – от 100 000 до 200 000 рублей; - для юрлица – от 1 млн. до 6 млн. рублей.	Ч. 8 ст. 13.11
Оператор не предоставил или несвоевременно предоставил в Роскомнадзор сведения	Штраф: - для должностных лиц – от 300 до 500 рублей; - для юрлица – от 3 000 до	Ст. 19.7

(либо в неполном объеме или в искаженном виде)	5 000 рублей.	