

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ПРОФСОЮЗНОЙ ОРГАНИЗАЦИИ



Основные нормативные правовые акты

- Конституция Российской Федерации – **статья 2**
- Европейская Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) [рус., англ.] (Заключена в г. Страсбурге 28.01.1981г.)
- Федеральный закон от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»
- **Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»**
- **Трудовой кодекс Российской Федерации – гл.14**

Персональные данные -

любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место его рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

(ст. 3 ФЗ «О персональных данных»)

Виды персональных данных

ОБЩИЕ: включают в себя любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) – фиио, дата рождения, место жительства, номер телефона, фотография, электронная почта и т.п. (п. 1 ст. 3 Закона о персональных данных).

СПЕЦИАЛЬНЫЕ: расовая и национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья (ч. 1 ст. 10 Закона о персональных данных).

БИОМЕТРИЧЕСКИЕ: сведения, на основе которых можно установить личность человека, характеризующие его физиологические особенности (ст. 11 Закона о персональных данных).

Используете пропуска с фотографиями? Получите письменное согласие!

К биометрическим персональным данным относятся физиологические данные (ч.1 ст.11 Закона о персональных данных):

дактилоскопические данные,

➤ радужная оболочка глаз,

➤ анализы ДНК,

➤ рост,

➤ вес,

➤ слепок голоса,

➤ отпечатки папиллярных узоров пальцев,

➤ изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для установления личности субъекта (Письмо Роскомнадзора от 29 августа 2022 г. N 08-78032)

Законно ли видеонаблюдение на рабочих местах?

Видеонаблюдение правомерно, если:

- ведется только для конкретных и заранее определенных правомерных целей, связанных с исполнением работником его обязанностей;
- работники поставлены в известность о ведении видеонаблюдения (так реализуется их право на получение полной и достоверной информации об условиях труда);
- видеонаблюдение ведется открыто — в помещениях, где установлены камеры, в зонах их видимости есть информационные таблички.

Документы, содержащие персональные данные:

- анкета, автобиография, личный листок по учету кадров, которые заполняются работником при приеме на работу.
- копия документа, удостоверяющего личность работника
- личная карточка № Т-2
- трудовая книжка или ее копия, трудовой договор
- копии свидетельств о заключении брака, рождении детей
- документы воинского учета
- справка о доходах с предыдущего места работы
- документы об образовании.
- документы обязательного пенсионного страхования.
- подлинники и копии приказов по личному составу
- при необходимости - иные документы, содержащие персональные данные работников

Обработка персональных данных -

это любое действие (операция) или совокупность действий (операций), совершаемых с использованием или без использования средств автоматизации, с персональными данными.

Обработка персональных данных осуществляется:

- с использованием средств автоматизации (с помощью средств вычислительной техники)
- без использования средств автоматизации (при непосредственном участии человека)

Обработка персональных данных без средств автоматизации

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. постановлением Правительства РФ от 15.09.2008 N 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»).

Обработкой ПД 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).

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.

Автоматизированная обработка персональных данных -

обработка данных с помощью средств вычислительной техники (программных комплексов - ИСПДн).

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.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (1С: ЗУП; 1С:Предприятие 3иК; Налогоплательщик ЮЛ; Парус; СУФД(казначейство); СводСмарт:сводная отчетность; Документооборот и делопроизводство и многие другие).

Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Оператор персональных данных

- государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (п. 2 ст. 3 Закона № 152-ФЗ)

Обработка персональных данных третьим лицом по поручению оператора

Основные признаки:

- наличие самостоятельной правосубъектности, то есть обработчик должен быть юридически независимым по отношению к оператору,
- обработка им персональных данных должна осуществляться в интересах оператора.

Обработчик не обязан получать согласие субъекта персональных данных на их обработку, поскольку ответственность перед гражданином за действия обработчика несет именно оператор

Способы защиты персональных данных

- **Правовые меры** защиты предполагают принятие локальных нормативных актов и организационно-распорядительных актов: политика обработки ПД, [?](#) положение о защите персональных данных и другие локальные нормативные акты.
- **Взаимодействие с Роскомнадзором** – еще один способ обеспечить защиту ПД.
- **Организационные меры** могут включать в себя назначение ответственных лиц, обучение работников, формирование культуры приватности в компании.
- **Меры технического характера** предусматривают выбор надежных поставщиков программного обеспечения и серверных мощностей, средств защиты информации, разработку технической документации в компании (технических заданий, моделей угроз), а также реализацию мер защиты данных при работе с программным обеспечением.

Основные обязанности работодателя (оператора) при работе с персональными данными (ст.ст.18.1,19 152-ФЗ)

- оценка случаев обработки персональных данных;
- разработка и принятие локальных нормативных актов, регламентирующих порядок обработки, включая вопросы хранения и использования персональных данных работников;
- назначение лица, ответственного за организацию обработки персональных данных;
- установление перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;
- организация хранения и обработки персональных данных (ст.ст. 86 - 87 ТК РФ);
- получение обязательства о нераспространении персональных данных от лиц, имеющих к ним доступ;
- ознакомление работников под подпись с Политикой и Положением об организации работы с персональными данными;

- письменное согласие работников на обработку персональных данных;
- обеспечение неограниченного доступа к Положению и Политике;
- первичное уведомление и дальнейшее взаимодействие с Роскомнадзором;
- внутренний контроль и аудит и т.д.
- ознакомление работников оператора, непосредственно осуществляющих обработку ПД, с законодательством о персональных данных, документами, определяющими политику оператора в отношении обработки ПД, локальными актами по вопросам обработки ПД;
- обучение указанных сотрудников;
- оценка вреда в соответствии с требованиями Роскомнадзора, который может быть причинен субъекту ПД;
- своевременное изменение, уничтожение, обезличивание ПД.

Локальные нормативные акты

- какие данные обрабатываются и с какой целью,
- кто субъекты персональных данных в компании,
- куда персональные данные передаются,
- какие информационные системы используются,
- как обеспечивается защита информационных систем,
- какой класс присваивается информационной системе,
- как хранятся документы, содержащие персональные данные,
- как осуществляется сбор персональных данных,
- как уничтожаются персональные данные и пр.

Политика обработки персональных данных

*(ст.18.1 Федерального закона 152-ФЗ,
Рекомендации по составлению документа, определяющего
политику оператора в отношении обработки персональных
данных, в порядке, установленном федеральным законом от 27
июля 2006г. № 152-ФЗ «О персональных данных».)*

- Общие положения
- Цели сбора персональных данных
- Правовые основания обработки персональных данных
- Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных
- Порядок и условия обработки персональных данных
- Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным

<https://rkn.gov.ru/personal-data/p908/>

Положение о защите о персональных данных

(2 ч.1 ст. 18.1 Закона №152-ФЗ)

- Общие положения (цели принятия Положения , предмет регулирования)
- Основные понятия. Состав персональных данных работников (документы, содержащие персональные данные)
- Обработка персональных данных (условия соблюдения обработки персональных данных)
- Передача персональных данных (порядок передачи персональных данных внутри организации, а также сторонним лицам и государственным органам)
- Доступ к персональным данным работников (информация о порядке доступа к персональным данным работников. Доступ внутренний и внешний)
- Ответственность за нарушение законодательства о персональных данных (кто конкретно в организации несет ответственность за нарушение правил хранения и использования персональных данных)

Надо ли уведомлять Роскомнадзор?

С 01.09.2022г. не требуется уведомлять Роскомнадзор об обработке персональных данных в случаях:

- обработки включенных в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- если оператор осуществляет деятельность по обработке персональных данных исключительно без использования средств автоматизации;
- предусмотренных законодательством о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

(п. 14 ст. 1 Федерального закона от 14.07.2022 N 266-ФЗ):

В остальных случаях необходимо уведомлять Роскомнадзор, в том числе, если обработка только в рамках трудовых отношений или для однократного пропуска на территорию!

Направить уведомление также можно на сайте Роскомнадзора:
<https://pd.rkn.gov.ru/operators-registry/notification/>

Предельный срок уведомления не определен.

Форма определена Приложением 1 к приказу Роскомнадзора от 28.10.2022 № 180

Проверьте, есть ли работодатель в реестре операторов: <https://pd.rkn.gov.ru/operators-registry/operators-list/>

Приказ Роскомнадзора от 30.05.2017 N 94 "Об утверждении методических рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения"

Уведомление рекомендуется оформляется:

- на бумажном носителе или
- в форме электронного документа.

Уведомление подписывается уполномоченным лицом.

Сведения об Операторе вносятся в Реестр не позднее 30 дней с даты регистрации Уведомления.

В случае изменения сведений оператор обязан уведомить Роскомнадзор не позднее 15-го числа месяца, следующего за месяцем, в котором возникли такие изменения

- **Приказ Роскомнадзора от 28 октября 2022 г. N 180 "Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных".**

- **Информация Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 25 декабря 2022 г. "Примеры заполнения документов об обработке персональных данных"**

Получение персональных данных

Основные принципы:

- соблюдение законодательства
- конфиденциальность
- личное согласие работника
- добровольность предоставления информации

Согласие должно быть конкретным, информированным и сознательным и однозначным.

Согласие на обработку персональных данных:

- Согласие на обработку персональных данных
- Согласие на обработку персональных данных, разрешенных работником для распространения

По новым правилам согласия на обработку персональных данных должны быть:

предметными, однозначными, конкретными, информированными и сознательными.

Согласие работника на обработку персональных данных включает:

- фамилию, имя, отчество, адрес работника, реквизиты документа, удостоверяющего его личность, включая дату выдачи и сведения о выдавшем его органе;
- при получении согласия от представителя работника - его фамилию, имя, отчество, адрес, реквизиты документа, удостоверяющего его личность, включая дату выдачи и сведения о выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия представителя;
- наименование или фамилию, имя, отчество и адрес работодателя;
- цель обработки персональных данных;
- перечень персональных данных, которые подлежат обработке;
- фамилию, имя, отчество и адрес лица или наименование организации, осуществляющих обработку персональных данных по поручению работодателя, если она поручена такому лицу или организации;
- перечень действий с персональными данными, на совершение которых работником дано согласие, общее описание способов их обработки;
- срок действия согласия работника на обработку его персональных данных, и способ отзыва согласия;
- подпись работника.

Не требуется согласие работника на передачу персональных данных:

- третьим лицам в целях предупреждения угрозы жизни и здоровью работника;
- в ФСС России, ПФР в объеме, предусмотренном законом;
- в налоговые органы ;
- в военные комиссариаты;
- по запросу профессиональных союзов в целях контроля за соблюдением трудового законодательства работодателем;
- по мотивированному запросу органов прокуратуры;
- по мотивированному требованию правоохранительных органов и органов безопасности;
- по запросу от государственных инспекторов труда при осуществлении ими надзорно-контрольной деятельности;
- в органы и организации, которые должны быть уведомлены о тяжелом несчастном случае, в том числе со смертельным исходом;
- в случаях, связанных с исполнением работником должностных обязанностей, в том числе при направлении в командировку.
- для предоставления сведений в банк, обслуживающий банковские карты работников.

Согласие на обработку персональных данных, разрешенных работником для распространения

- фамилия, имя, отчество (при наличии) субъекта персональных данных;
- контактная информация (номер телефона, адрес электронной почты или почтовый адрес субъекта персональных данных);
- сведения об операторе - наименование, адрес, указанный в Едином государственном реестре юридических лиц, идентификационный номер налогоплательщика, основной государственный регистрационный номер (если он известен субъекту персональных данных);
- сведения об информационных ресурсах оператора;
- цель (цели) обработки персональных данных;
- категории и перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- категории и перечень персональных данных, для обработки которых субъект персональных данных устанавливает условия и запреты;
- условия, при которых полученные персональные данные могут передаваться оператором, осуществляющим обработку персональных данных, только по его внутренней сети, обеспечивающей доступ к информации лишь для строго определенных сотрудников, либо с использованием информационно-телекоммуникационных сетей, либо без передачи полученных персональных данных (заполняется по желанию субъекта персональных данных);
- срок действия согласия;
- подпись работника.

Получение персональных данных работника у третьих лиц

Письменное согласие работника обязательно в форме уведомления, в котором указываются:

- цели получения персональных данных работника у третьего лица;
- предполагаемые источники информации (лица, у которых будут запрашиваться данные);
- способы получения данных, их характер;
- возможные последствия отказа работодателю в получении персональных данных работника у третьего лица.

Неправомерная передача персональных данных!!!

Оператор при обнаружении факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных ч. 3.1 ст. 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» **обязан уведомить Роскомнадзор:**

- ❑ в течение **24 часов** о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- ❑ в течение **72 часов** о результатах **внутреннего расследования** выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Обращаем внимание, что указанная форма предназначена для направления информации оператором персональных данных о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных.

Если работник полагает, что **нарушены его права**, как субъекта персональных данных, следует воспользоваться формой для направления обращения в Роскомнадзор, размещенной по ссылке: <https://rkn.gov.ru/treatments/ask-question/>

Уничтожение персональных данных -

это один из видов обработки персональных данных, в результате которого становится невозможным восстановить содержание ПД в информационной системе или уничтожаются материальные носители.

Правила подтверждения факта уничтожения персональных данных утверждены приказом Роскомнадзора от 28.10.2022 № 179

Акт об уничтожении персональных данных

- наименование организации или ФИО предпринимателя и их адрес местонахождения;
- ФИО лиц, чьи персональные данные были уничтожены;
- ФИО и должность лица, уничтожившего персональные данные, а также его подпись;
- перечень категорий уничтоженных персональных данных;
- наименование уничтоженного материального носителя, содержащего персональные данные, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных вручную);
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные (в случае их обработки на компьютере);
- способ уничтожения персональных данных;
- причину уничтожения данных и дату уничтожения.

Выгрузка из журнала регистрации должна содержать:

- ФИО лиц, чьи персональные данные были уничтожены;
- перечень категорий уничтоженных персональных данных;
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные;
- причину уничтожения персональных данных
- дату их уничтожения

Хранение персональных данных

- Федеральный закон от 22.10.2004 N 125-ФЗ (ред. от 14.07.2022) "Об архивном деле в Российской Федерации"
- Приказ Федерального Архивного агентства от 20 декабря 2019 г. N 237 «Об утверждении Инструкции по применению перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»
- Приказ Росархива от 20.12.2019 N 236 "Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения"
- Приказ Росархива от 02.03.2020 N 24 (ред. от 26.09.2022) "Об утверждении Правил организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных и муниципальных архивах, музеях и библиотеках, научных организациях"

Права работников в области защиты персональных данных:

- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

Продолжение

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением законодательства;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- отзыв согласия на обработку персональных данных;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Ответственность работодателя за нарушение законодательства о ПД

Административная ответственность 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.

- **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.

- Работодатель несет **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).

- Нарушение законодательства о защите персональных

данных может повлечь **уголовную ответственность** (ч. 1 ст. 137, ч. 1 ст. 272 УК РФ, п.3 Постановления Пленума Верховного Суда РФ от 15.12.2022 N 37, ст. 140 УК

Ответственность работника за нарушение законодательства о ПД

- **Дисциплинарная ответственность**

Разглашение персональных данных – основание увольнения по пп. "в" п. 6 ч. 1 ст. 81 ТК РФ (подтверждено судебной практикой).

- **Материальная ответственность**

Если работник нарушил свои обязанности и причинил тем самым ущерб (ст.90, ч. 1 ст. 238 ТК РФ)

Распространенные нарушения требований законодательства по ПД

- Неполный перечень целей обработки ПД, самих ПД, категорий субъектов, правовых оснований (ФЗ № 152 им не является), нарушения при составлении согласия на обработку ПД;
- Отсутствие адреса базы ПД либо неполный перечень адресов баз;
- Непредоставление в РКН сведений о прекращении обработки ПД или об изменении информации, содержащейся в уведомлении;
- Непринятие мер, необходимых для обеспечения выполнения обязанностей, предусмотренных ФЗ № 152;
- Отсутствие мест хранения ПД (материальных носителей);
- Несоблюдение требований по информированию лиц, осуществляющих обработку ПД без использования средств автоматизации.

Спасибо за внимание

Ведущий юрисконсульт
Правовой инспекции труда
Аппарата МФП,

Илькина Надежда Анатольевна
8(495) 688-48-00
unona@bk.ru