

**ПЕРСОНАЛЬНЫЕ
ДАННЫЕ
РАБОТНИКОВ**

Персональными данными является

любая информация, прямо или косвенно относящаяся к субъекту персональных данных - определенному или определяемому физическому лицу (ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных")

- фамилия, имя, отчество;
- пол, возраст;
- изображение человека (фотография и видеозапись), которое позволяет установить личность и с этой целью используется оператором (Разъяснения Роскомнадзора «О вопросах отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки»);
- 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.

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 N Т-2.
- трудовая книжка или ее копия.
- копии свидетельств о заключении брака, рождении детей.
- документы воинского учета.
- справка о доходах с предыдущего места работы.
- документы об образовании.
- документы обязательного пенсионного страхования.
- трудовой договор.
- подлинники и копии приказов по личному составу.
- при необходимости - иные документы, содержащие персональные данные работников.

Право работников на защиту своих персональных данных

Согласно ст. 89 ТК РФ, имеют право на свободный бесплатный доступ к своим персональным данным, в том числе на получение копии любой записи, содержащей такие данные.

Учитывая требования ст. 62 ТК РФ, по письменному заявлению работника работодатель обязан не позднее трех рабочих дней со дня получения от работника заявления выдать ему копии документов, связанных с работой

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Обработка персональных данных - это любое действие (операция), совершаемых с использованием или без использования средств автоматизации, с персональными данными, включая:

- сбор,
- запись,
- систематизацию,
- накопление,
- хранение,
- уточнение (обновление, изменение),
- извлечение,
- использование,
- передачу (распространение, предоставление, доступ),
- обезличивание,
- блокирование,
- удаление,
- уничтожение персональных данных.

Требования к обработке

1. обработка должна осуществляться на законной и справедливой основе;
2. обработка должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка, несовместимая с целями сбора персональных данных;
3. не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
4. обработке подлежат только те персональные данные, которые отвечают целям обработки;
5. содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Не допускается обработка избыточных данных по отношению к заявленным целям обработки;
6. при обработке должны быть обеспечены точность и достаточность персональных данных, а в необходимых случаях - актуальность по отношению к целям обработки. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;
7. форма хранения персональных данных должна позволять определять субъекта этих данных. Хранение не должно длиться дольше, чем этого требуют цели обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Доказать получение согласия работника
на обработку его персональных данных
должен

работодатель !

Согласие работника на обработку его персональных данных

ПРИМЕР:

письменное согласие работника
на обработку его персональных данных требуется

1. при получении персональных данных работника у третьей стороны (п. 3 ст. 86 ТК РФ). Подробнее об этом см. п. 2 настоящего материала;
2. при передаче персональных данных работника третьим лицам, кроме тех случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, а также в иных предусмотренных федеральными законами случаях (абз. 2 ст. 88 ТК РФ);
3. для обработки специальных категорий персональных данных работника, непосредственно связанных с вопросами трудовых отношений (п. 4 ст. 86 ТК РФ, п. 1 ч. 2 ст. 10 Закона о персональных данных).

Согласие работника на обработку персональных данных должно включать

1. фамилию, имя, отчество, адрес работника, реквизиты документа, удостоверяющего его личность, включая дату выдачи и сведения о выдавшем его органе;
2. 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;
3. наименование или фамилию, имя, отчество и адрес работодателя;
4. цель обработки персональных данных;
5. перечень персональных данных, которые подлежат обработке;
6. фамилию, имя, отчество и адрес лица или наименование организации, осуществляющих обработку персональных данных по поручению работодателя, если она поручена такому лицу или организации;
7. перечень действий с персональными данными, на совершение которых работником дано согласие, общее описание способов их обработки;
8. срок, в течение которого действует согласие работника на обработку его
9. персональных данных, и способ отзыва согласия;
10. подпись работника.

ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Все персональные данные работника следует получать у него самого (п. 3 ст. 86 ТК РФ).

Причем это допускается только с его согласия (п. 1 ч. 1 ст. 6 Федерального закона от 27.07.2006 N 152-ФЗ).

Не требуется согласие

- из документов (сведений), предъявляемых при заключении трудового договора;
- по результатам обязательного предварительного медицинского осмотра о состоянии здоровья;
- в объеме, предусмотренном унифицированной формой N Т-2, в том числе персональных данных близких родственников, и в иных случаях, установленных законодательством РФ (получение алиментов, оформление допуска к государственной тайне, оформление социальных выплат)
- от кадрового агентства, действующего от имени соискателя;
- из резюме соискателя, размещенного в сети Интернет и доступного неограниченному кругу лиц.

ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок хранения и использования персональных данных работников устанавливается работодателем

Журнал учета персональных данных

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

Требования к помещению, где хранятся персональные данные

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

Защита персональных данных

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 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.

ОТВЕТСТВЕННОСТЬ ПРИМЕНЯЕТСЯ К РАБОТОДАТЕЛЯМ

ДИСЦИПЛИНАРНАЯ ОТВЕТСТВЕННОСТЬ

За дисциплинарный проступок сбора, обработки и хранения персональных данных работодатель может наказать своего работника, применив к нему одно из следующих взысканий (ч.1 ст. 192 ТК РФ):

- замечание;
- выговор;
- увольнение.

МАТЕРИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ

Материальная ответственность работника может наступить, если в связи с нарушением правил работы с персональными данными организации причинен прямой действительный ущерб (ст. 238 ТК РФ).

Взыскание причиненного ущерба можно осуществить по распоряжению руководителя не позднее одного месяца со дня окончательного установления размера причиненного сотрудником ущерба.

АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ

За нарушение порядка сбора, хранения, использования или распространения персональных данных работодателя и должностных лиц контролирующие органы могут привлечь к административной ответственности в виде штрафов, которые могут составлять:

- для должностных лиц: от 500 до 1000 рублей;
- для организации: от 5000 до 10 000 рублей.

Отдельный (самостоятельный) штраф для должностных лиц за разглашение персональных данных в связи с исполнением служебных или профессиональных обязанностей составляет от 4000 до 5000 рублей.

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ

Уголовная ответственность для директора, главного бухгалтера или начальника отдела кадров компании или другого лица, ответственного за работу с персональными данными, может наступить за незаконные действия:

- сбор или распространение сведений о частной жизни сотрудника, составляющих его личную или семейную тайну, без его согласия;
- распространение сведений о работнике в публичном выступлении, публично демонстрирующемся произведении или СМИ.

Меры уголовной ответственности

- штраф до 200 000 рублей (или в размере доходов осужденного за период до 18 месяцев);
- обязательные работы на срок до 360 часов;
- исправительные работы на срок до одного года;
- принудительные работы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового;
- арест на срок до четырех месяцев;
- лишение свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет.

ЧТО ИЗМЕНИЛОСЬ С 1 ИЮЛЯ 2017 ГОДА

Федеральный закон от 07.02. 2017 № 13-ФЗ расширил перечень оснований для привлечения работодателя к административной ответственности в области защиты персональных данных, а также увеличил размеры административных штрафов.

Сразу скажем, что административная ответственность в сфере персональных данных существенно ужесточена. При этом важно следующее: вместо единственного вида административной ответственности, описанного в статье 13.11 КоАП РФ, появится семь

НАРУШЕНИЕ 1: ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В «ИНЫХ» ЦЕЛЯХ

Обработка персональных данных в случаях, не предусмотренных законодательством, либо обработка персональных данных, несовместимая с целями сбора персональных данных – самостоятельные виды административного нарушения

(ч. 1 ст. 13.11 КоАП РФ).

Пример

Организация-работодатель собирает персональные данные работников и передает эти данные сторонним компаниям в рекламных целях (передаются ФИО, телефоны, регионы проживания, уровень дохода).

Потом рекламные фирмы начинают рассылать работникам на телефон, e-mail и домашние адреса различный спам и рекламные предложения.

Если в таких действиях работодателя не будет выявлено уголовного состава преступления, то можно будет применить административную ответственность

Наказание

1. Предупреждение;

2. Штрафы

- на граждан - в размере от 1000 до 3000 руб.;
- на должностных лиц – 5000 до 10 000 руб.;
- на юридических лиц – от 30 000 до 50 000 руб.

НАРУШЕНИЕ 2: ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ СОГЛАСИЯ

С 1 июля 2017 года обработка персональных данных без согласия работника в письменной форме, либо если письменное согласие не содержит обозначенных выше сведений – это самостоятельное административное нарушение, предусмотренное в части 2 статьи 13.11 КоАП РФ.

За него возможны штрафные санкции:

- на граждан - в размере от 3000 до 5000 руб.;
- на должностных лиц (например, директор, кадровик или ИП) – от 10 000 до 20 000 руб.;
- на организации - от 15 000 до 75 000 руб.

НАРУШЕНИЕ 3: ДОСТУП К ПОЛИТИКЕ ПО ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор, осуществляющий сбор персональных данных в Интернете (например, через сайт), обязан опубликовать в Интернете документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу.

С выполнением этой обязанности на практике сталкиваются многие пользователи сети Интернет. Так, например, когда вы оставляете какую-либо заявку на сайтах и указываете свои ФИО и e-mail, то можете обратить внимание на ссылку на подобные документы: «Политика обработки персональных данных», «Положение об обработке персональных данных» и т.п. Однако стоит признать, что некоторые сайты этим пренебрегают и никакой ссылки не приводят. И получается, что человек оставляет заявку на сайте, не знает, в каких целях сайт собирает персональные данные.

Некоторые работодатели также на своих сайтах выставляют имеющиеся вакансии и предлагают кандидатам заполнить форму «О себе».

Наказание

С 1 июля 2017 года в части 3 статьи 13.11 КоАП РФ выделен самостоятельный состав правонарушения – невыполнение оператором обязанности по публикации или предоставлению неограниченного доступа к документу с политикой по обработке персональных данных или сведениями по их защите.

Ответственность по этой статье может выглядеть как предупреждение или административные штрафы:

- на граждан - от 700 до 1500 руб.;
- на должностных лиц (например, директора или главбуха) - от 3000 до 6000 руб.;
- на индивидуальных предпринимателей - от 5000 до 10 000 руб.;
- на организации - от 15 000 до 30 000 руб.

НАРУШЕНИЕ 4: СОКРЫТИЕ ИНФОРМАЦИИ

Субъект персональных данных (то есть, физическое лицо, кому принадлежат эти данные) имеет право на получение информации, касающейся обработки его персональных данных.

С 1 июля 2017 года невыполнение оператором обязанности по предоставлению субъекту персональных данных информации, касающейся обработки его персональных данных, является самостоятельным административным нарушением.

Оно влечет предупреждение или наложение административных штрафов

- на граждан – от 1000 до 2000 руб.;
- на должностных лиц (например, директора, кадровика или бухгалтера) - от 4000 до 6000 руб.;
- на индивидуальных предпринимателей – 10 000 до 15 000 руб.;
- на юридических лиц (организаций) – от 20 000 до 40 000 руб.

НАРУШЕНИЕ 5: УТОЧНЕНИЯ ИЛИ БЛОКИРОВКА

Статья 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» предусматривает, что в ряде случаев оператор обязан уточнять, блокировать или уничтожать персональные данные физических лиц.

С 1 июля 2017 года введен новый вид административного нарушения – невыполнение оператором требования субъекта персональных данных или его представителя об уточнении, блокировке, уничтожении данных (если данные неполные, устаревшие, неточные, незаконно получены или не являются необходимыми для заявленной цели обработки).

Такие действия с 1 июля 2017 года влекут предупреждение или наложение административных штрафов:

- на граждан - от 1000 до 2000 руб.;
- на должностных лиц (например, директора, кадровика или главбуха) - от 4000 до 10 000 рублей;
- на ИП - от 10 000 до 20 000 рублей;
- на юридических лиц – 25 000 до 45 000 руб.

НАРУШЕНИЕ 6: СОХРАННОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

Многие работодатели собирают персональные данные работников только «на бумаге» и не ведут никакой автоматизированной обработки, не имеют специальных программ для обработки и баз данных.

С 1 июля 2017 года законодатели выделили для таких операторов (в частности, работодателей) новый вид правонарушения за необеспечение оператором при обработке персональных данных без использования средств автоматизации обязанности по сохранности персональных данных при хранении их материальных носителей, если это привело к неправомерному или случайному доступу к персональным данным.

А это, в свою очередь, послужило причиной их уничтожения, изменения, блокирования, копирования, предоставления, распространения либо иного неправомерного действия.

Если это произошло, то административная ответственность может наступить в виде административного штрафа:

- на граждан - 700 до 2000 руб.;
- на должностных лиц (например, руководителя) - от 4000 до 10 000 руб.;
- на индивидуальных предпринимателей - от 10 000 до 20 000 руб.;
- на организаций – от 25 000 до 50 000 руб.

НАРУШЕНИЕ 6: ОБЕЗЛИЧИВАНИЕ

В исключительных случаях, предусмотренных законодательством, государственные и муниципальные органы должны обезличивать персональные данные, которые обрабатывают в своих информационных системах, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ (подп. «з» п. 1 перечня, утвержденного постановлением Правительства РФ от 21 марта 2012 г. № 211).

К таким случаям относится, например, необходимость государственных и муниципальных органов размещать в открытом доступе документы, содержащие персональные данные, допустим, обезличенные копии судебных актов

ПРИВЛЕКАТЬ К ОТВЕТСТВЕННОСТИ СТАНЕТ ПРОЩЕ

До 1 июля 2017 года возбуждать дела по административным делам, связанным с персональными данными, по статье 13.11 КоАП РФ был вправе исключительно прокурор.

С 1 июля 2017 года участие прокурора будет необязательным.

С указанной даты дела по статье 13.11 КоАП будут вправе возбуждать должностные лица Роскомнадзора.

Такая поправка внесена комментируемым законом в пункт 58 части 2 статьи 28.3 КоАП РФ. Следовательно, процедура привлечения к ответственности по делам о персональных данных становится проще.

Пример 1.

Должностное лицо без согласия человека разгласил зарплату, премию, вознаграждение по договору, передал данные должников в юридическую фирму, чтобы составить исковые заявления или разместил копию заявления человека в качестве образца на стенде с образцами других заявлений.

С 1 июля 2017 г. инспекторы Роскомнадзора квалифицируют такое нарушение как разглашение персональных данных без письменного согласия от человека или по письменному согласию, которое оформлено с нарушениями и выдадут постановление об административном правонарушении и назначат штраф: на учреждение – от 15 000 до 75 000 руб., на должностное лицо – от 10 000 до 20 000 руб. (ч. 2 ст. 13.11 КоАП РФ).

Пример 2.

Бухгалтер не предоставил сотруднику расчетный листок, справку, сведения о страховом стаже и другие документы, в которых есть персонифицированные сведения о человеке.

С 1 июля 2017 г. инспекторы Роскомнадзора квалифицируют такое нарушение как сокрытие от человека его персональных данных и назначат штраф: на учреждение – от 20 000 до 40 000 руб., на бухгалтера – от 4000 до 6000 руб. (ч. 4 ст. 13.11 КоАП РФ).

Пример 3.

Должностное лицо отказался принять к обработке новые паспортные данные человека, банковские реквизиты или другую изменяющую информацию –

за такое нарушение инспекторы могут назначить штраф на учреждение – от 25 000 до 45 000 руб, а на должностное лицо – от 4000 до 10 000 руб

Пример 4.

Должностное лицо небрежно работает с документами, персональные сведения о сотруднике стали известны другим лицам из-за того, что он оставил на столе без присмотра или вынес с рабочего места справки, расчетные листки, другие документы с персональными данными или потерял эти документы.

С 1 июля 2017 г. инспекторы Роскомнадзора квалифицируют такое нарушение как невыполнение требования человека уточнить, заблокировать или уничтожить его персональные данные и назначат штраф:

на учреждение – от 25 000 до 50 000 руб., а на бухгалтера – от 4000 до 10 000 руб. (ч. 6 ст. 13.11 КоАП РФ).

Пример 5.

Должностное лицо передает имена, адреса, телефоны и другие данные сотрудников организациям, действующим в рекламных целях, коллекторским агентствам или другим третьим лицам.

С 1 июля 2017 г. инспекторы Роскомнадзора квалифицируют такое нарушение как обработку персональных данных, когда это не предусмотрено законами и не соответствуют целям сбора персональных данных и назначат штраф на учреждение – от 30 000 до 50 000 руб., а на бухгалтера – от 5000 до 10 000 руб. (ч. 1 ст. 13.11 КоАП РФ).

Консалтинговая группа КонсалтФинансАудит

Генеральный директор Дегтярева Светлана Львовна

Тел. +7(4852)585210,+7(4852)207075

kfaaudit@yandex.ru