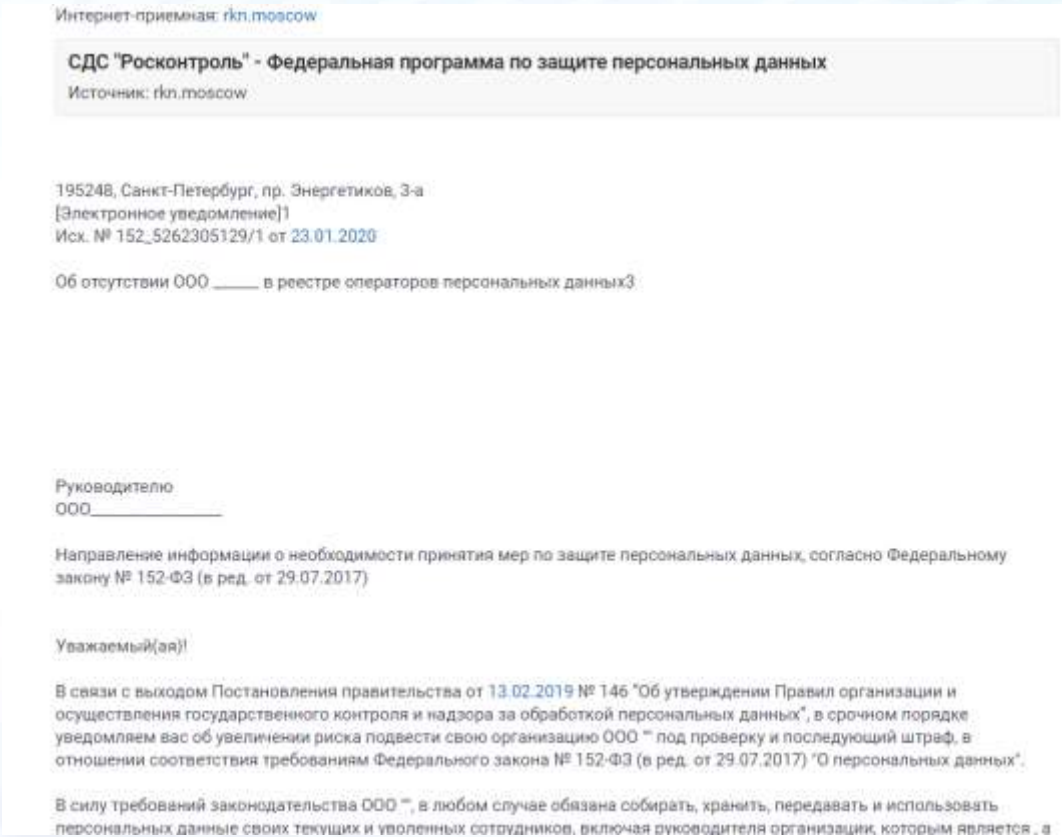
Общие требования по организации обработки персональных данных на предприятии

РОСКОМНАДЗОР

Пермь, 2021

Внимание! Массовая рассылка писем от имени Роскомнадзора!



Интернет-приемная: rkn.moscow

СДС "Росконтроль" - Федеральная программа по защите персональных данных

Источник: rkn.moscow

195248, Санкт-Петербург, пр. Энергетиков, 3-а
[Электронное уведомление]1
Исх. № 152_5262305129/1 от 23.01.2020

Об отсутствии ООО _____ в реестре операторов персональных данных3

Руководителю
ООО_____

Направление информации о необходимости принятия мер по защите персональных данных, согласно Федеральному закону № 152-ФЗ (в ред. от 29.07.2017)

Уважаемый(ая)!

В связи с выходом Постановления правительства от 13.02.2019 № 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных", в срочном порядке уведомляем вас об увеличении риска подвести свою организацию ООО "" под проверку и последующий штраф, в отношении соответствия требованиям Федерального закона № 152-ФЗ (в ред. от 29.07.2017) "О персональных данных".

В силу требований законодательства ООО "", в любом случае обязана собирать, хранить, передавать и использовать персональных данные своих текущих и уволенных сотрудников, включая руководителя организации, которым является , а

РОСКОМНАДЗОР

Не переходите по ссылкам, указанным в таких письмах, не вступайте с отправителями в переписку и не заказывайте платных услуг у сторонних компаний. Имейте ввиду: организациям, индивидуальным предпринимателям или физическим лицам не нужны посредники для подачи данных в Роскомнадзор.

Перечень основных нормативных правовых актов в целях обработки персональных данных работников и иных лиц на предприятиях

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
2. Глава 14 Трудового Кодекса Российской Федерации.
3. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
4. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
5. Приказ (распоряжение) по предприятию «О назначении ответственного за организацию обработки персональных данных».
6. Утверждённые руководителем предприятия «Правила обработки персональных данных, обработки персональных данных, **устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований».**

РОСКОМНАДЗОР

Разберём некоторые понятия данные в ст. 3 ФЗ «О персональных данных»

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

любая информация

относящаяся прямо или косвенно

к определенному или определяемому физическому лицу

ОПЕРАТОР

государственный орган, муниципальный орган, юридическое или физическое лицо

самостоятельно или совместно с другими лицами

организующие и (или) осуществляющие обработку персональных данных

определяющие: цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

В силу понятия «персональные данные», данного в ст. 3 ФЗ «О персональных данных», а также определений указанных в ст. 10 и ст. 11 данного закона персональные данные формально можно разделить на следующие три группы

ОБЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- ☑ Фамилия, Имя, Отчество
- ☑ Дата рождения
- ☑ Место жительства
- ☑ Номер телефона
- ☑ Фотография
- ☑ Электронная почта

СПЕЦИАЛЬНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- ☑ Рассовая и национальная принадлежность
- ☑ Религиозные и филосовские убеждения
- ☑ Состояние здоровья

БИОМЕТРИЧЕСКИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- ☑ Отпечатки папилярных узоров пальцев
- ☑ Рисунок радужной оболочки глаз
- ☑ Термограмма лица
- ☑ ДНК
- ☑ Слепок голоса

РОСКОМНАДЗОР

Обработка персональных данных - ***любое действие (операция) или совокупность действий (операций***), совершаемых с использованием средств автоматизации или без использования таких средств с ПД, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу распространение, предоставление, удаление.

Распространение персональных данных - действия, направленные на их раскрытие ***неопределенному кругу лиц***.

Предоставление персональных данных - действия, направленные на их раскрытие персональных данных ***определенному лицу*** или определенному кругу лиц.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

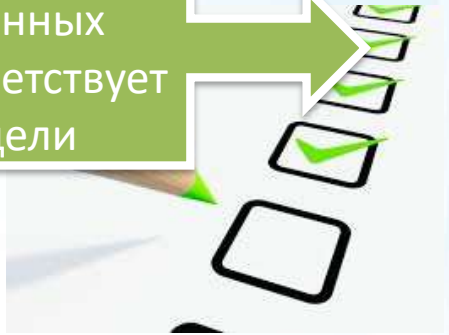
Объём данных соответствует цели

Цель 1

Цели определены заранее и законны

Цель 2

Содержание данных соответствует цели



Заранее определённый срок наступил – возможность идентификации субъекта исключается

Объединение баз данных с разными целями не допускается

Цель достигнута – данные уничтожаются

РОСКОМНАДЗОР

Требования к работодателю при обработке персональных данных работников (гл. 14 ТК РФ)

- 1) обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- 2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, настоящим Кодексом и иными федеральными законами;
- 3) все персональные данные работника следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение;

- 4) работодатель не имеет права получать и обрабатывать сведения о работнике, относящиеся к специальным категориям персональных данных, за исключением случаев, предусмотренных настоящим Кодексом и другими федеральными законами;
- (5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных настоящим Кодексом или иными федеральными законами;
- 6) при принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- 7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном настоящим Кодексом и иными федеральными законами;
- 8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;
- 9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

Давайте разберём случаи, при наступлении которых допускается обработка персональных данных (включая предоставление, раскрытие) без согласия субъектов персональных данных, установлены п.п. 2-11 ч. 1 ст. 6 ФЗ «О персональных данных»).

РОСКОМНАДЗОР

2) Закон
3) Суд
3.1) исполнение судебного акта
4) оказание государственных и муниципальных услуг
5) обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных + для заключения договора по инициативе субъекта персональных данных
6) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно

7) Взыскание задолженности (230-ФЗ)
8) обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности СМИ либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных;
9) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением агитации и продвижения товаров
10) - персональные данные, сделанные общедоступными субъектом персональных данных (*действия данного пункта заканчиваются 31.03.2021 в связи с вступлением в силу ст. 10.1 Закона*)
11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Разберём случаи когда необходимо согласие работника на обработку его персональных данных

Получение согласия в письменной форме обязательно в следующих случаях:

1) **Трансграничная передача ПД**
2) **Биометрические ПД**
3) **Специальные категории ПД**
4) **При включении персональных данных в общедоступные источники персональных данных**
5) **При решении, порождающем юридические последствия в отношении субъекта персональных данных, может быть принято на основании исключительно автоматизированной обработки его персональных данных**

При этом , содержание такого согласия должно соответствовать перечню сведений, содержащихся в нём, предусмотренным ч. 4 ст. 9 ФЗ «О персональных данных»

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме.

Например:
-заявление о приёме на работу с заполненной анкетой или автобиографией (кроме органов власти);
-получение бонусной карты у лица оказывающего услуги (автозаправки, детский мир и т.д.), в части заполненной анкеты-заявления на получение такой карты;
-заявление о приёме для получения платной медицинской услуги и т.д.

В соответствии со ст. 7 ФЗ «О персональных данных»
Работодатель и должностные лица предприятия, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

С согласия субъекта

Предусмотрено федеральным законом

С 31.03.2021 в силу вступает ст. 10.1 ФЗ «О персональных данных», в которой в частности определены «Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения», при этом, согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

ЧТО нужно сделать на предприятии, чтобы соответствовать требованиям законодательства в области персональных данных???

1. Назначить ответственного за организацию обработки персональных данных.

2. Разработать документы, определяющие политику в отношении обработки ПД, локальные акты по вопросам обработки ПД.

3. Ознакомить работников с положениями законодательства о персональных данных, с локальными актами оператора

4. Уведомить Роскомнадзор о своем намерении осуществлять обработку персональных данных.

РОСКОМНАДЗОР

5. Принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие привлекаемыми лицами для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации указаны в Постановлении Правительства РФ от 15.09.2008 № 687.

Требования к защите персональных данных при их обработке в информационных системах персональных данных и уровни защищенности таких данных, установлены постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Обязанности ответственного за организацию обработки персональных данных

- Лицо, ответственное за организацию обработки персональных данных, в частности, обязано:
- ***1) осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;***
- 2) доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- 3) организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

Осуществление внутреннего контроля

- Как правило, приложением к правилам ОПД (Положение) являются Правила осуществления внутреннего контроля соответствия
- обработки персональных данных требованиям к защите
- персональных данных в _____(указывается наименование оператора.
- Указанные Правила включают в себя следующее:
- - ***процедуры, направленные на выявление*** и предотвращение нарушений законодательства РФ в сфере персональных данных;
- - ***основания, порядок, формы и методы проведения*** внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Наиболее характерные нарушения

- Обработка персональных данных без уведомления уполномоченного органа.
- Отсутствие у оператора места (мест) хранения персональных данных (материальных носителей), перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.
- Сотрудники не ознакомлены с положением об обработке персональных данных (для всех сотрудников организации),инструкциями (только для участвующих в обработке).
- Обработка персональных данных (в том числе хранение) после достижения целей обработки.
- Отсутствие политики в отношении обработки персональных данных.
-Не назначен ответственный за организацию обработки персональных данных.

Уполномоченный орган по защите прав субъектов персональных данных введет реестр операторов

Оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных (ст. 22 ФЗ «О персональных данных») если кто-то ещё не сделал этого воспользуйтесь телефоном указанным ниже.

Pd.rkn.gov.ru

РОСКОМНАДЗОР

Консультации по телефону: **258-15-37 (доб. 534)**

Телефоны для консультаций:

258-15-37 – по заполнению уведомлений и информационных писем

258-15-35 или 258-15-36 – по вопросам обработки персональных данных

Благодарю за внимание!