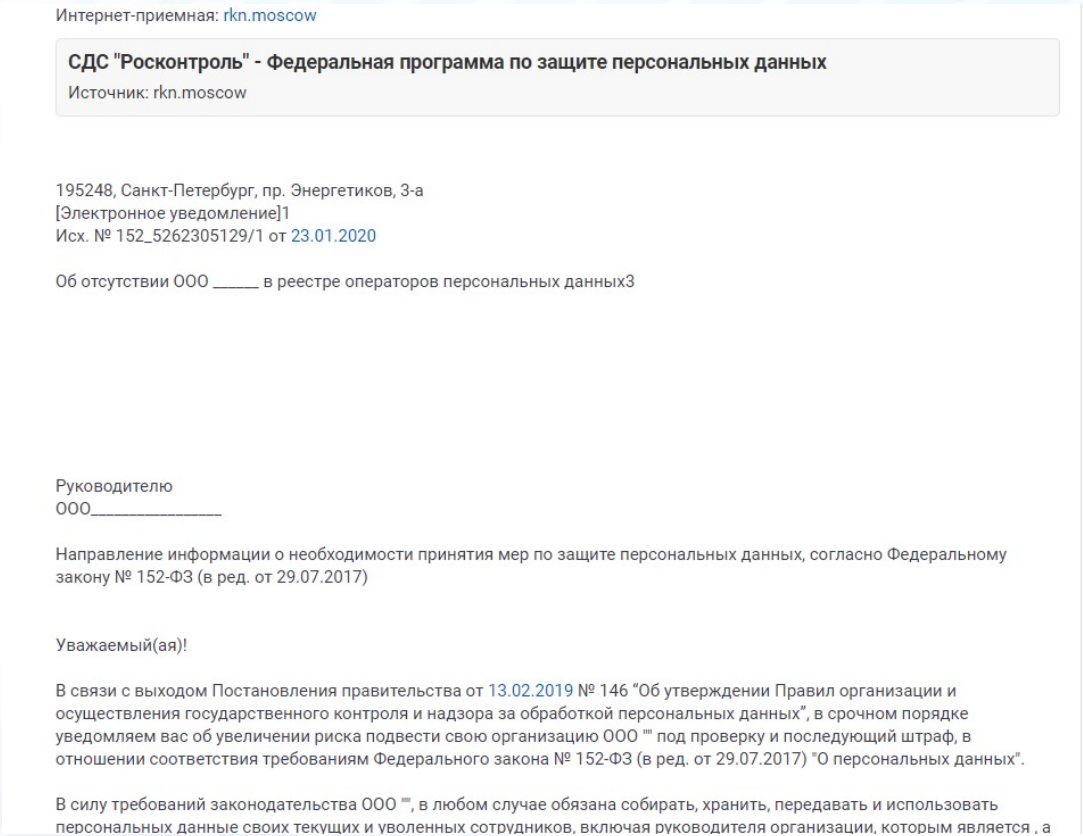
Об основах обработки персональных данных в организациях, учреждениях, предприятиях

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

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.

РОСКОМНАДЗОР

Перечень основополагающих нормативных правовых актов

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
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».

Законодательство в области персональных - структура и особенности

- Федеральный закон «О персональных данных» не относится к основаниям для обработки персональных данных в организациях, учреждениях, предприятиях, органах власти и иных структурах, а лишь определяет:
- **-сферы действия закона, так например, закон не распространяется на отношения, связанные с** обработкой пд физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных; организации хранения, комплектования, учета и использования содержащих персональные данные документов Архивного фонда РФ в соответствии со 125-ФЗ; пд, отнесенных к сведениям, составляющим гос.тайну;
- -основные понятия в области ПД ;
- -принципы и условия обработки персональных данных:
- -права субъектов пд, обязанности Операторов, осуществляющих обработку пд и др.

Примерный перечень нормативных актов, являющихся основанием для ОПД в организациях, учреждениях и т.д.

- 1. Устав предприятия, организации, учреждения.
- 2. Глава 14 Трудового Кодекса Российской Федерации.
  3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
  4. Утверждённые руководителем предприятия:
  - Политика по обработке персональных данных,
  - Правила (Положение) обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства РФ в сфере ПД, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых ПД, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований».
-

Принципы и условия обработки ПД

- обработка должна осуществляться на законной и справедливой основе и ***ограничиваться достижением конкретных, заранее определенных и законных целей***. Не допускается обработка ПД, несовместимая с целями их сбора;
- ***не допускается объединение баз данных***, содержащих ПД, обработка которых осуществляется в целях, несовместимых между собой;
- обрабатываемые ПД ***не должны быть избыточными по отношению к заявленным целям их обработки***;
- должны быть ***обеспечены точность ПД, их достаточность***, а в необходимых случаях и актуальность по отношению к целям обработки;
- ***хранение ПД должно осуществляться в форме, позволяющей определить субъекта ПД***, не дольше, чем этого требуют цели обработки, если срок хранения не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект.

ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ ПД

- 1) **персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 1.1) **персональные данные, разрешенные субъектом персональных данных для распространения**, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом;
- 2) **оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ ПД

- 3) **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;
- 4) **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
- 5) **распространение п**ерсональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 6) **предоставление** персональных данных - действия, направленные **на раскрытие персональных** данных определенному лицу или определенному кругу лиц;
- 7) **блокирование** персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ ПД

- 8) **уничтожение** персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;
- 9) **обезличивание** персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
- 10) **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- 11) **трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

По понятиям , данным в ст. 3, ст. 10, ст. 11 ФЗ «О персональных данных» их можно разделить на следующие категории ПД

- **Общие ПД** - информация, которую можно отнести к определённому или определяемому физическому лицу, в частности ФИО; данные документа удостоверяющего личность; данные водительского удостоверения; адрес регистрации; сведения о месте проживания, учёбе, работе и др., **позволяющие посредством простого выбора данных отнести их к определённому лицу.**
- **Специальные категории ПД** - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, сведений о судимости, то есть это любые сведения касающиеся ЛИЧНОЙ жизни физического лица.
- **Биометрические ПД** – это сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором ***для установления личности субъекта персональных данных (отпечатки пальцев, термограмма лица и т.д.)***

О СОГЛАСИИ НА ОБРАБОТКУ ПД

- ***Обработка ПД любого гражданина, в том числе работника может осуществляться:***
- А. в случаях, предусмотренных законом **только с письменного согласия**.

- Б. **с согласия**, данного субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

- В. **без согласия** гражданина, в случаях, предусмотренных ч. 1 ст. 6 ФЗ «О персональных данных».

Случаи, при наступлении которых допускается обработка персональных данных (включая предоставление, раскрытие) без согласия субъектов персональных данных, установлены п.п. 2-10 ч. 1 ст. 6 ФЗ «О персональных данных»).

РОСКОМНАДЗОР

2) В соответствии с законом (например: в целях оказания мед услуг)
3) в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах
3.1) в целях исполнение судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством РФ об исполнительном производстве
4) в целях оказания 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 (ЦЕЛЬ!!!)
11) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

Согласие субъекта на обработку его персональных данных

В письменной форме, при этом форма должна соответствовать ч. 4 ст. 9 ФЗ «О персональных данных», которая предусматривает 6 случаев:

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

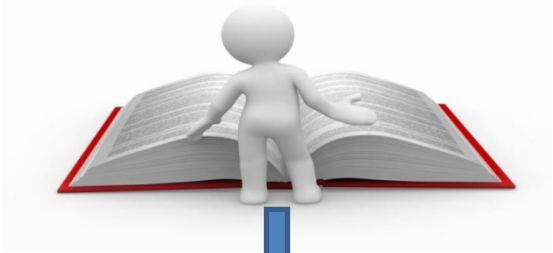
С согласия субъекта

Предусмотрено федеральным законом

НОВЕЛЛА: С 31.03.2021 в силу вступили требования 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.

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»)



Pd.rkn.gov.ru

РОСКОМНАДЗОР

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

- **Какие действия необходимо совершить на предприятиях в целях исполнения обязанностей, предусмотренных законодательством 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.

5. Принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

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.

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 в соответствии с законодательством Российской Федерации в области персональных данных 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;

10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

Основные нарушения, выявленные в ходе плановых проверок.

- **ч. 3 ст. 6** ФЗ «О персональных данных» поручение обработки персональных данных без согласия субъекта;

- **ч. 1 ст. 22** ФЗ «О персональных данных» (Обработка персональных данных без уведомления уполномоченного органа);

- **ч. 1 ст. 18.1** ФЗ «О персональных данных» (не назначен ответственный за организацию обработки персональных данных, отсутствие политики в отношении обработки персональных данных, сотрудники не ознакомлены с положением об обработке персональных данных (для всех сотрудников организации), инструкциями (только для участвующих в обработке);

- **ч. 7 ст. 22** ФЗ «О персональных данных» (несвоевременное непредставление сведений об изменениях в реестр операторов, осуществляющих ОПД);

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.

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.

Статья 13.11. Нарушение законодательства РФ в области ПД

1. *ОПД в случаях, не предусмотренных законодательством РФ в области ПД, либо ОПД, несовместимая с целями сбора ПД*, - влечет наложение административного штрафа ***на граждан вот двух тысяч до шести тысяч рублей; на ДЛ - от десяти тысяч до двадцати тысяч рублей; на ЮЛ - от шестидесяти тысяч до ста тысяч рублей***.

1.1. **Повторное** - ***на граждан от четырех тысяч до двенадцати тысяч рублей; на ДЛ - от двадцати тысяч до пятидесяти тысяч рублей; на ИП - от пятидесяти тысяч до ста тысяч рублей; на ЮЛ- от ста тысяч до трехсот тысяч рублей***.

2. ОПД без согласия **в письменной форме** субъекта ПД на обработку его ПД в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ в области ПД, за исключением случаев, предусмотренных статьей 17.13 (**Незаконное распространение сведений о защищаемых лицах)**, либо ОПД с нарушением установленных законодательством РФ в области ПД требований к составу сведений, включаемых в согласие в письменной форме субъекта ПД на обработку его ПД, - ***штраф на граждан от шести тысяч до десяти тысяч рублей; на ДЛ - от двадцати тысяч до сорока тысяч рублей; на ЮЛ - от тридцати тысяч до ста пятидесяти тысяч рублей***.

Статья 13.11. Нарушение законодательства РФ в области ПД

2.1. ***Повторное*** - на граждан в размере от десяти тысяч до двадцати тысяч рублей; на ДЛ - от сорока тысяч до ста тысяч рублей; на ИП - от ста тысяч до трехсот тысяч рублей; на ЮЛ - от трехсот тысяч до пятисот тысяч рублей.

3. Невыполнение оператором предусмотренной законодательством РФ в области ПД обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, ***определяющему политику оператора в отношении обработки ПД***, или сведениям о реализуемых требованиях к защите ПД - штраф на граждан от одной тысячи пятисот до трех тысяч рублей; на ДЛ - от шести тысяч до двенадцати тысяч рублей; на ИП - от десяти тысяч до двадцати тысяч рублей; на ЮЛ - от тридцати тысяч до шестидесяти тысяч рублей.

4. Невыполнение оператором предусмотренной законодательством РФ в области ПД обязанности по предоставлению субъекту ПД информации, касающейся обработки его ПД, - штраф на граждан от двух тысяч до четырех тысяч рублей; на ДЛ - от восьми тысяч до двенадцати тысяч рублей; на ИП - от двадцати тысяч до тридцати тысяч рублей; на ЮЛ - от сорока тысяч до восьмидесяти тысяч рублей.

Статья 13.11. Нарушение законодательства РФ в области ПД

2.1. ***Повторное*** - на граждан в размере от десяти тысяч до двадцати тысяч рублей; на ДЛ - от сорока тысяч до ста тысяч рублей; на ИП - от ста тысяч до трехсот тысяч рублей; на ЮЛ - от трехсот тысяч до пятисот тысяч рублей.

3. Невыполнение оператором предусмотренной законодательством РФ в области ПД обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, ***определяющему политику оператора в отношении обработки ПД***, или сведениям о реализуемых требованиях к защите ПД - штраф на граждан от одной тысячи пятисот до трех тысяч рублей; на ДЛ - от шести тысяч до двенадцати тысяч рублей; на ИП - от десяти тысяч до двадцати тысяч рублей; на ЮЛ - от тридцати тысяч до шестидесяти тысяч рублей.

4. Невыполнение оператором предусмотренной законодательством РФ в области ПД обязанности по предоставлению субъекту ПД информации, касающейся обработки его ПД, - штраф на граждан от двух тысяч до четырех тысяч рублей; на ДЛ - от восьми тысяч до двенадцати тысяч рублей; на ИП - от двадцати тысяч до тридцати тысяч рублей; на ЮЛ - от сорока тысяч до восьмидесяти тысяч рублей.

Статья 13.11. Нарушение законодательства РФ в области ПД

2.1. ***Повторное*** - на граждан в размере от десяти тысяч до двадцати тысяч рублей; на ДЛ - от сорока тысяч до ста тысяч рублей; на ИП - от ста тысяч до трехсот тысяч рублей; на ЮЛ - от трехсот тысяч до пятисот тысяч рублей.

3. Невыполнение оператором предусмотренной законодательством РФ в области ПД обязанности по опубликованию или обеспечению иным образом неограниченного доступа к документу, ***определяющему политику оператора в отношении обработки ПД***, или сведениям о реализуемых требованиях к защите ПД - штраф на граждан от одной тысячи пятисот до трех тысяч рублей; на ДЛ - от шести тысяч до двенадцати тысяч рублей; на ИП - от десяти тысяч до двадцати тысяч рублей; на ЮЛ - от тридцати тысяч до шестидесяти тысяч рублей.

4. Невыполнение оператором предусмотренной законодательством РФ в области ПД обязанности по предоставлению субъекту ПД информации, касающейся обработки его ПД, - штраф на граждан от двух тысяч до четырех тысяч рублей; на ДЛ - от восьми тысяч до двенадцати тысяч рублей; на ИП - от двадцати тысяч до тридцати тысяч рублей; на ЮЛ - от сорока тысяч до восьмидесяти тысяч рублей.

Телефоны для консультаций:

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

258-15-35 (36) – по вопросам обработки персональных данных

Благодарю за внимание!