Разъяснения законодательства в сфере защиты прав субъектов персональных данных

**Вопрос:** **Что относится к персональным данным?**

**Ответ:**Это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Например: его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес места жительства, паспортные данные, образование, место работы, должность, доходы, ИНН, данные военного билета, СНИЛС, медицинского полиса, сведения о движимом и недвижимом имуществе, о ценных бумагах и кредитных обязательствах, сведения о вкладах в банках и номера счетов, сведения о состоянии здоровья, о судимости, сведения о членах семьи (о детях) и так далее.

**Вопрос:** **Какие действия являются обработкой персональных данных?**

**Ответ:**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.

**Вопрос:** **Кто является оператором персональных данных?**

**Ответ:**Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных. При этом операторами указанные органы и лица являются независимо от включения в реестр операторов, осуществляющих обработку персональных данных, который ведет Роскомнадзор.

**Вопрос: Является ли обработкой персональных данных размещение на сайтах в сети Интернет фотографии без иной дополнительной информации?**

**Ответ:**Размещение на страницах сайтов в сети Интернет фотографии без дополнительной информации, позволяющей идентифицировать физическое лицо как субъекта персональных данных, не может свидетельствовать об обработке персональных данных конкретного физического лица.

**Вопрос: Является ли обработкой персональных данных размещение фамилии, имени и отчества без иной дополнительной информации?**

**Ответ:**Размещение на страницах сайтов в сети Интернет фамилии, имени и отчества без дополнительной информации, позволяющей идентифицировать физическое лицо как субъекта персональных данных, не может свидетельствовать об обработке персональных данных конкретного физического лица.

**Первоочередные задачи оператора персональных данных по организации обработки персональных данных**

**1.** Проверить, как ведется в организации обработка ПД на данный момент, устранить выявленные нарушения, не ждать проверки надзирающего органа исполнительной власти.

**2.** Подготовить требуемую действующим законодательством в области персональных данных документацию по обработке ПД, разработать инструкции для сотрудников, довести. Разработать (уточнить в соответствии с новой редакцией 152-ФЗ и подзаконными актами) и утвердить положение об обработке ПД в организации.

**3.** Получить согласие субъектов ПД на обработку ПД (в случаях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в соответствии с ч. 4 ст. 9).

**4.** Утвердить списки лиц, допущенных к обработке ПД.

**5.** Довести до сотрудников, которые допущены к обработке ПД:

- факт допуска их к обработке ПД;

- о способе обработки ПД;

- о перечне категорий персональных данных, которые они будут обрабатывать.

 Обязать работников (сотрудников), обрабатывающих ПД, обеспечить безопасность обработки ПД.

**6.** Обеспечить надежное хранение носителей ПД.

**7.** Зарегистрироваться в установленном порядке в Реестре операторов ПД.

**8.** Дополнить договоры с организациями, которым оператор поручил обработку ПД, перечнем действий (операций) с ПД, целями обработки ПД,  обязанностью обеспечения конфиденциальности при обработке ПД переданных им для выполнения условий данного договора, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

**9.** Привести в соответствие с требованиями действующего законодательства в области персональных данных деятельность по обработке ПД (если этого ещё не сделано).

**10.** Организовать периодический контроль руководства организации за работой  лиц, допущенных к обработке персональных данных.

**11.** Проверить порядок хранения документов, содержащих персональные данные, и порядок их уничтожения по достижению цели обработки этих персональных данных.

**12.** Представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в пунктах 5, 7.1, 10 и 11 части 3 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»:

- п.5 ч.3 ст.22 – правовое основание обработки персональных данных;

- п.7.1. ч.3 ст.22 – фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных (это, например,  ЕРЦ, РИЦ, объединённые бухгалтерии – то есть обработчик персональных данных, который не определяет цели обработки персональных данных), и номера их контактных телефонов, почтовые адреса и адреса электронной почты;

- п.10 ч.3 ст.22 – сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

- п.11 ч.3 ст.22 – сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленные Правительством Российской Федерации (ст.19 ещё не установлены! С июня 2012).

13. Представить в уполномоченный орган по защите прав субъектов персональных данных сведения, указанные в пункте 10.1 части 3 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» - «Сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации».

**Типичные ошибки**

**при заполнении уведомлений об обработке персональных данных**

В ходе рассмотрения представленных в Управление Роскомнадзора по Уральскому федеральному округ в 2007 – 2015 гг. уведомлений об обработке персональных данных и информационных писем о внесении изменений в реестр операторов, осуществляющих обработку персональных данных, выявлены следующие типичные ошибки при их заполнении:

**В поле «Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных»**

Операторы не указывают конкретный перечень действий с персональными данными:

- Сбор, анализ, обобщение, хранение, изменение, дополнение, передача, уничтожение персональных данных.

И их конкретные способы обработки:

- неавтоматизированная обработка персональных данных;

- исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;

- смешанная обработка персональных данных с передачей полученной информации по сети или без таковой.

Наиболее частая ошибка – **отсутствие либо нечеткое указание на порядок передачи информации при смешанной и (или) автоматизированной обработке**.

Необходимо четко указать соответствующие варианты:

«информация передается по внутренней сети юридического лица»

«информация не передается по внутренней сети юридического лица»

«информация доступна лишь для строго определенных сотрудников»

«информация передается с использованием сети общего доступа Интернет»

«без передачи полученной информации»

**В поле «Дата начала обработки персональных данных»**

Операторы не указывают дату вообще или только год, или неверные данные

Необходимо указать **конкретную фактическую дату** (число, месяц, год) начала совершения действий с персональными данными.

**В поле «Описание мер, предусмотренных статьями 18.1 и 19 Федерального закона «О персональных данных»**

При заполнении данного поля уведомления либо вообще отсутствует описание мер, либо нет их четкого раскрытия

Необходимо указать **конкретные** **организационные и технические меры**, в том числе использование шифровальных (криптографических) средств для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий при их обработке.

**К организационным мерам** можно отнести:

- принятие локальных нормативных актов (внутренних документов – приказов, положений, регламентов, перечней сведений и т.д.) организации;

- разграничение сотрудников к информации с персональными данными.

**К техническим мерам** можно отнести:

- защита от несанкционированного физического доступа к информации (обеспечение охраны всех помещений – физическая или иная),

- ограничение доступа к компьютерной технике для определенных категорий работников,

При смешанной обработке указывается перечень мер по обеспечению безопасности персональных данных **на бумажных носителях и на электронных носителях (и возможно по специально выделенной сети Интернет).**

**К средствам обеспечения безопасности** можно отнести:

 - защита от несанкционированного физического доступа к информации (хранение персональных данных в закрытых шкафах, ящиках, сейфах),

- наличие лицензионных программных средств защиты.

**В поле «Цель обработки персональных данных»**

Необходимо указать как цели, **указанные в учредительных документах** (уставе, учредительном договоре, положении) оператора, так и **цели фактически осуществляемой оператором деятельности**.

Например:

- «осуществление полномочий органа власти по ….»

- «выполнение государственных функций по ….»

- «оказание государственных (муниципальных) услуг по …»

- «оказание (предоставление) услуг по ….»

- «выполнение работ по ….»

- «осуществление … деятельности …»

Соответствующие виды деятельности отражаются в общероссийских классификаторах услуг, видов деятельности (ОКУН, ОКВЭД) и т.д.

**В поле «Категории персональных данных»**

Операторы зачастую указывают фразы типа «и др.», «и т.п.» «другая информация».

Необходимо указывать **все конкретные** категории, например:

фамилия, имя, отчество, год, месяц, дата рождения, место рождение, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, расовая принадлежность, национальная принадлежность, политические взгляды, религиозные убеждения, философские убеждения, состояние здоровья, состояние интимной жизни;

биометрические персональные данные (сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность - данные изображения отпечатка пальца, изображения лица, изображения радужной оболочки глаза и т.д.);

А также другие категории персональных данных в соответствии с наличием полученных копий документов или информации из них от субъектов персональных данных.

**В поле «категории субъектов, персональные данные которых обрабатываются»**

Операторы указывают **не все категории субъектов**, при этом из текста уведомления видно, что обрабатываются данные других категорий.

Например: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (оператором); физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором) и др.

**В поле «Правовое основание обработки персональных данных»**

Операторы не указывают соответствующие статьи и номер закона или иного нормативно-правового акта, регулирующих осуществляемый вид деятельности и касающихся обработки персональных данных.

**В поле «Срок или условие прекращения обработки персональных данных»**

Операторы не заполняют данное поле вообще

Необходимо указать конкретную дату или основание (условие), наступление которого повлечет прекращение обработки персональных данных – например «ликвидация юридического лица», «аннулирование лицензии на осуществление соответствующего вида деятельности»

**В поле «Наименование (фамилия, имя, отчество), адрес оператора»**

Типичные ошибки в данном случае:

- не указан (не полностью указан) адрес оператора (например, не указаны почтовый индекс, муниципальный район (для организаций районов области), улица, номер дома, корпус – если имеются), ИНН

- несоответствие полного наименования организации на бланке и (или) печати и в уведомлении. А также несоответствие с учредительными документами. Необходимо точное соответствие!

**А так же:**

- Уведомление исполняется не на бланке организации;

- не сообщается номер и ключ к электронной форме уведомления;

- не сообщаются контактные данные исполнителя;

- подписывается не лицом имеющим право подписи документов.