Приложение 2

Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных

Настоящие Рекомендации разработаны в целях установления единых принципов и порядка заполнения уведомления об обработке (о намерении осуществлять обработку) персональных данных (далее - Уведомление).

**Уведомление оформляется на бланке оператора** (по форме, прилагаемой к настоящим Рекомендациям), осуществляющего обработку персональных данных (далее - оператор), **и направляется в территориальный орган Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций** (далее - территориальный орган Роскомнадзора).

Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации.

**1**. В поле **«Наименование (фамилия, имя, отчество), адрес оператора»** указывается:

**1.1**. ***Для операторов - юридических лиц***:

- полное наименование с указанием организационно-правовой формы и сокращенное наименование юридического лица (оператора), осуществляющего обработку персональных данных;

- наименование филиала(ов) (представительства(в) юридического лица (оператора), осуществляющего обработку персональных данных <1>;

- место нахождения (юридический адрес) <2>;

- почтовый адрес (фактический адрес),

 - индивидуальный номер налогоплательщика (ИНН),

-ОГРН, КПП, ОКОПФ, ОКВЭД, ОКПО, ОКОГУ, ОКФС,

- вид субъекта предпринимательства (отношение к микропредприятию, малому, среднему, крупному предприятию - Федеральный закон № 209-ФЗ от 24.07.2007г. «О развитии малого и среднего предпринимательства в Российской Федерации».

**1.2**. ***Для операторов - физических лиц:***

- фамилия, имя, отчество физического лица (оператора);

- местонахождение <3>;

-------------------------

<**1**> Для юридических лиц с филиальной структурой указывается список субъектов Российской Федерации (с указанием кода субъекта - согласно справочнику «Коды регионов», утвержденному Приказом ФНС России от 13.10.2006 N САЭ-3-04/706@ «Об утверждении формы сведений о доходах физических лиц», зарегистрированным Министерством юстиции Российской Федерации 17.11.2000, регистрационный номер 8507), на территории которых находятся филиалы (представительства) юридического лица и (или) где оператором производится обработка персональных данных. Уведомление направляется юридическим лицом в соответствующее территориальное управление Роскомнадзора по месту своего нахождения с указанием всех имеющихся филиалов (представительств).

<**2**> Указывается место нахождения юридического лица в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, а также место нахождения филиалов (представительств) юридического лица, контактная информация.

Для организаций, учреждений, имеющих филиалы (представительства), указываются юридический и фактический адрес (как юридического лица, так и его филиалов и представительств), где осуществляется непосредственная обработка персональных данных (все действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных). При этом необходимо уточнить - обработка персональных данных осуществляется только юридическим лицом (формирование центральной информационной системы) и (или) филиалами (представительствами).

<**3**> Указывается местонахождение физического лица в соответствии со свидетельством о постановке на учет физического лица в налоговом органе, почтовый адрес, контактная информация.

Данные документа, удостоверяющего личность, дата его выдачи, наименование органа, выдавшего документ;

- индивидуальный номер налогоплательщика (ИНН).

**1.3**. ***Для индивидуальных предпринимателей***:

- фамилия, имя, отчество индивидуального предпринимателя (оператора);

- место жительства <4>;

- индивидуальный номер налогоплательщика (ИНН).

**1.4**. ***Для государственных, муниципальных органов (операторов):***

- полное и сокращенное наименование государственного, муниципального органа;

- наименование территориального(ых) органа(ов), осуществляющего(их) обработку персональных данных;

- место нахождения <5>;

- индивидуальный номер налогоплательщика (ИНН).

При указании наименования (фамилии, имени, отчества), адреса оператора, а также направления деятельности рекомендуется использовать также ссылки на код(ы) классификаторов (ОКОПФ, ОКВЭД, ОКПО, ОКОГУ, ОКОП, ОКФС).

**2**. В поле **«Правовое основание обработки персональных данных»** указываются**:**

Федеральный закон, постановление Правительства Российской Федерации, иной нормативно-правовой акт, закрепляющий основание и порядок обработки персональных данных (Примечание № 1);

номер, дата выдачи и наименование лицензии на осуществляемый вид деятельности с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных (Примечание № 2), Устав (Положение), утвержденный от «дата».

**3**. В поле **«Цель обработки персональных данных»** указываются цели обработки персональных данных (а также их соответствие полномочиям оператора) (Примечание № 3).

-----------------------------

<**4**> Указывается место жительства индивидуального предпринимателя (оператора) в соответствии с данными документа, удостоверяющего личность, и свидетельством о постановке индивидуального предпринимателя на учет в налоговом органе, почтовый адрес, контактная информация.

<**5**> Указывается место нахождения государственного, муниципального органа в соответствии с учредительными документами и свидетельством о постановке юридического лица на учет в налоговом органе, почтовый адрес государственного, муниципального органа, контактная информация.

**Примечание № 1**: Указываются не только соответствующие статьи Федерального закона «О персональных данных», но и статьи иного нормативно-правового акта, регулирующие осуществляемый вид деятельности и касающиеся обработки персональных данных. (Например: ст. ст. 86 - 90 Трудового кодекса РФ, ст. 85.1 Воздушного кодекса РФ, ст. 12 Федерального закона «Об актах гражданского состояния» и др.)

**Примечание № 2:** Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу персональных данных (или информации, касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных условий.

**Примечание № 3**: под «Целью обработки персональных данных» понимаются как цели, указанные в учредительных документах оператора (уставе, учредительном договоре, положении), так и цели фактически осуществляемой оператором деятельности по обработке персональных данных. Например: «осуществление полномочий органа власти по …», «выполнение государственных функций по …», «оказание государственных (муниципальных) услуг по …», «выполнение работ по …», «осуществление … деятельности…». Соответствующие виды деятельности отражаются в общероссийских классификаторах услуг, видов деятельности (ОКУН, ОКВЭД) и т.д.

**4**. В поле **«Осуществляет обработку следующих категории персональных данных»** указываются все категории персональных данных, подлежащих обработке:

**4.1**. **Персональные данные** - любая информация, относящаяся к определенному или определяемому на основе такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы, и другие категории персональных данных, обрабатываемые оператором, не указанные в настоящем пункте.

**4.2**. **Специальные категории персональных данных** (расовая принадлежность, национальная принадлежность, политические взгляды, религиозные убеждения, философские убеждения, состояние здоровья, состояние интимной жизни).

**4.3.** **Биометрические персональные данные** (сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность) (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных).

**5.** В поле **«Принадлежащих следующим категориям субъектов»** указываются категории субъектов (физических лиц) и виды отношений с субъектами (физическими лицами), персональные данные которых обрабатываются. ***Например***: работники (субъекты), состоящие в трудовых отношениях с юридическим лицом (оператором), физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.) (субъекты), состоящие в договорных и иных гражданско-правовых отношениях с юридическим лицом (оператором) и др.

**6**. В поле **«Обработка вышеуказанных персональных данных осуществляется следующим путем:…»**

**а)** оператор указывает действия (операции) которые им применяются при обработке персональных данных. ***Перечень действий с персональными данными указан в п. 3 ст. 3 ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение.***

**б)** указываются действия, совершаемые оператором с персональными данными, а также описание используемых оператором способов обработки персональных данных:

- неавтоматизированная обработка персональных данных;

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

- смешанная обработка персональных данных (Примечание № 4). При *смешанной обработке* указывается перечень мер по обеспечению безопасности персональных данных на *бумажных носителях и на электронных носителях.*

***Указывается****:* ***передаются******(или******не передаются)******персональные данные по внутренней сети юридического лица, по сети Интернет****.*

7. В поле **«Для обеспечения безопасности персональных данных принимаются следующие меры:**

------------------------------

**Примечание №4**: При автоматизированной обработке персональных данных либо смешанной обработке необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети юридического лица (информация доступна лишь для строго определенных сотрудников юридического лица), либо информация передается с использованием сети общего пользования Интернет, либо без передачи полученной информации.

 **а) описание мер, предусмотренных ст.ст. 18.1 и 19 Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;**

 **б) сведения о наличии шифровальных (криптографических) средств и наименование этих средств;**

 **в) фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных и номера их контактных телефонов, почтовые адреса и адреса электронной почты лица».**

оператор указывает:

**а)** описание мер, предусмотренных ст.ст. 18.1 и 19 федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименование этих средств;

оператор обязан принять следующие меры (ст.18.1):

- назначить ответственного за обработку персональных данных (утвердить инструкции ответственных за обработку персональных данных);

- разработать Положение и Политику оператора в отношении обработки персональных данных;

- осуществлять внутренний контроль и аудит соответствия обработки персональных данных законодательству;

- произвести оценку вреда, который может быть причинен субъектам из-за нарушений ФЗ;

- ознакомить работников, обрабатывающих персональных данных, с законодательством о персональных данных, с Положением и Политикой оператора в отношении обработки персональных данных, внутренними документами по данной тематике и (или) провести их обучение под роспись;

(ст.19):

\*) оператор обязан 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.

\*\*) обеспечение безопасности достигается, в частности если:

- разработать модель актуальных угроз;

- использовать только сертифицированные средства защиты информации;

- провести оценку эффективности мер по обеспечению безопасности персональных данных (под этим подразумевается аттестация или декларирование соответствия);

- организовать учет машинных носителей;

- осуществлять резервное копирование персональных данных;

- установить правила доступа к персональных данных в информационную систему персональных данных (для этого необходимо разработать документы, регламентирующие доступ к персональным данным в системе); вести учет всех действий, совершаемых с персональными данными в информационной системе;

- вести контроль за мерами по обеспечению безопасности персональных данных (для этого необходимо регулярно проводить внутренние проверки).

 **б)** **фамилию, имя, отчество** физического лица или сотрудника юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты (***ст.22.1 Федерального Закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»***);

 **в)** **класс информационной системы** персональных данных оператора (пункт 14 приказа ФСТЭК России, ФСБ России. Мининформсвязи России от 13.02.2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»);

**г) *организационные и технические меры***, принимаемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, персональных данных:

к ***организационным мерам*** можно отнести: принятие локальных нормативных актов (внутренних документов – приказов, положений, регламентов, перечней сведений и т.д.) организации;

к ***техническим мерам*** *(средства обеспечения безопасности)*можно отнести:

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

- защита паролем компьютеров с персональными данными,

- использование системы паролей при работе в сети (портале),

- ограничение доступа к компьютерной технике для определенных категорий работников.

В случае использования оператором, осуществляющим обработку персональных данных, **шифровальных (криптографических) средств** указываются следующие сведения:

а) наименование, регистрационный номер, производитель используемых криптографических средств;

б) уровень криптографической защиты персональных данных;

в) уровень специальной защиты от утечки по каналам побочных излучений и наводок;

г) уровень защиты от несанкционированного доступа.

Представление данной информации осуществляется в соответствии с Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра Федеральной службы безопасности Российской Федерации 21 февраля 2008 г. № 149/5-144».

**8**. В поле **«Сведения о наличии или об отсутствии трансграничной передачи персональных данных»** указываются сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки с указанием перечня иностранных государств, на территорию которых обеспечивается трансграничная передача персональных данных.

**9**. В поле **«Сведения об обеспечении безопасности персональных данных» -** указываются сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации – с соответствием с ПП РФ от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», ПП РФ от 06.07.2008г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», ПП РФ от 01.11.2012г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», ПП РФ от 21.03.2012г. №211 «Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним актами, операторами, являющимися государственными или муниципальными органами».

**10.** В поле **«Дата начала обработки персональных данных»** указывается конкретная дата (число, месяц, год) начала совершения действия (операции) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных (фактическая дата начала обработки персональных данных).

**11**. В поле **«Срок или условие прекращения обработки персональных данных»** указывается конкретная дата (число, месяц, год) или основание (условие), наступление которого повлечет прекращение обработки персональных данных (в основном – ликвидация). ***Например,*** условиемпрекращения обработки ПД может быть ликвидация (прекращение деятельности) юридического лица, а датой прекращения обработки ПД – дата окончания действия имеющейся лицензии на осуществление вида деятельности при условии ее дальнейшего не продления.