«Работа с персональными данными»

Главный специалист отдела ОМиСЗИ ГАУ РК «ЦИТ»
Русанов Александр Владимирович
a.v.rusanov@cit.rkomi.ru

Сыктывкар, 2017 год

Краткое содержание

- ✔ *Ответственность, предусмотренная в 2017 г. за нарушение требований в области защиты персональных данных;*
- ✔ *Какие меры необходимо обязательно предпринять, в рамках построения системы защиты персональных данных в 2017 г.;*
- ✔ *Кто обеспечивает контроль и надзор за исполнением требований федерального законодательства в области защиты персональных данных;*
- ✔ *Что необходимо знать о проверках и органах, уполномоченных на проведение подобных мероприятий;*
- ✔ *Наиболее распространенные нарушения в области защиты персональных данных, выделенные Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Коми.*

Используемые сокращения

***ИСПДн** – информационные системы;*

***ОГВ** – орган государственной власти;*

***ОМСУ** – орган местного самоуправления;*

***ПДн** – персональные данные;*

***ПП** – постановление правительства;*

***СКЗИ** – средства криптографической защиты информации;*

***ФЗ** – федеральный закон;*

«Ответственность»

Ранее

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

- предупреждение
- Административный штраф
  - Физ. лица 300 – 500
  - Должн. лица 500 – 1000
  - Юр. лица 5 000 – 10 000

Статья 19.5. Невыполнение в срок законного предписания (постановления, представления, решения) органа (должностного лица), осуществляющего государственный надзор (контроль), организации, уполномоченной в соответствии с федеральными законами на осуществление государственного надзора (должностного лица), органа (должностного лица), осуществляющего муниципальный контроль

- Физ. лица 300 – 500
- Должн. лица 1 000 – 2 000 (дисквалификация 3 г.)
- Юр. лица 10 000 – 20 000

С 1 июля 2017 года

Федеральный закон от 07.02.2017 13-ФЗ «О внесении изменений в кодекс РФ об административных правонарушениях», вносящий поправки в КоАП.

Ст. 13.11. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ

- *7 наиболее распространенных нарушений, в сфере обработки ПДн;*
- *Штрафы до 15 000 для физических лиц;*
- *Штрафы до 68 000 для должностных лиц;*
- *Штрафы до 65 000 для индивидуальных предпринимателей;*
- *Штрафы до 290 000 для юридических лиц;*

Обработка ПДн в случаях, не предусмотренных законодательством РФ, или обработка ПДн, несовместимых с целями обработки

- *В согласии на обработку ПДн должна быть указана 1 цель обработки ПДн, в соответствии с которой осуществляется сбор ПДн;*
- *В согласии на обработку ПДн, должны быть указаны только те категории ПДн, которые реально необходимы для достижения конкретной цели, в противном случае данные будут считаться излишними, что является нарушением.*

ч.1. Ст. 13.11.

Обработка ПДн без письменного согласия в случаях, когда оно должно быть по закону

Условия, при которых не требуется брать согласие с субъектов ПДн описаны в ***ст. 6 Федерального закона от 27.07.2006 N 152-ФЗ***

- *Обработка ПДн необходима для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей (**п.2 . ч.1**);*
- *Обработка персональных данных необходима для исполнения полномочий ОГВ, ОМСУ и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных ФЗ от 27.07.2010 г. 210-ФЗ (**п.4. ч.1**);*
- *Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем (**п.5. ч.1**);*
- *Осуществляется обработка персональных данных, сделанных общедоступным субъектом персональных данных (п.10);*

ч.2. Ст. 13.11.

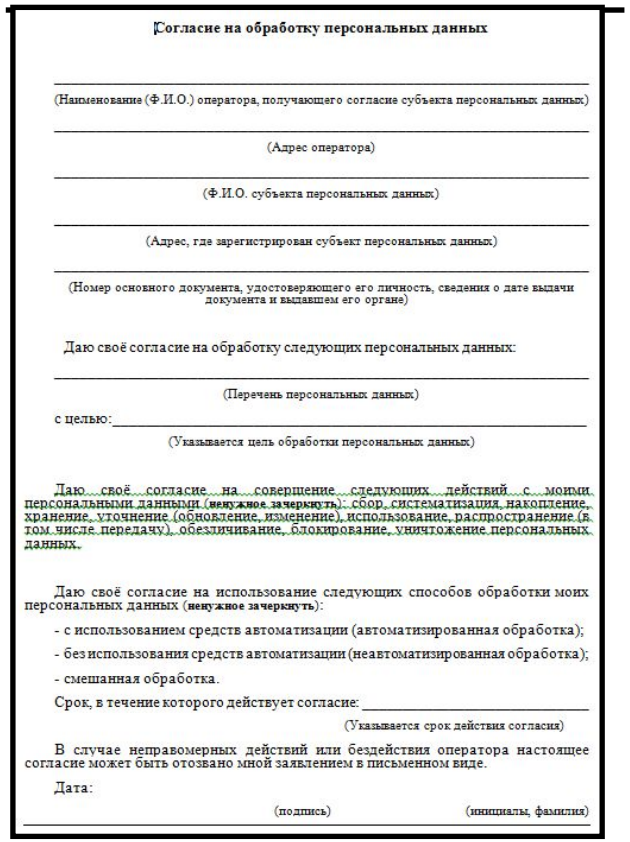
Письменное согласие на обработку ПДн

ч.4. Ст. 9. Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных».
Согласие на обработку ПДн в обязательном порядке включает:

- *ФИО, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;*
- *ФИО, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);*
- *наименование или ФИО и адрес оператора, получающего согласие субъекта ПДн;*
- *цель обработки персональных данных;*
- *перечень ПДн, на обработку которых дается согласие субъекта ПДн;*
- *наименование или ФИО и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;*
- *перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;*
- *срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;*
- *подпись субъекта ПДн.*

Примерная форма письменного согласия на обработку ПДн

На Интернет-страницах Управлений Роскомнадзора размещены примерные формы письменного согласия субъекта ПДн на обработку своих ПДн.



Согласие на обработку персональных данных

_____

(Наименование (Ф.И.О.) оператора, получающего согласие субъекта персональных данных)

_____

(Адрес оператора)

_____

(Ф.И.О. субъекта персональных данных)

_____

(Адрес, где зарегистрирован субъект персональных данных)

_____

(Номер основного документа, удостоверяющего его личность, сведения о дате выдачи документа и выдавшем его органе)

Даю своё согласие на обработку следующих персональных данных:

_____

(Перечень персональных данных)

с целью:_____

(Указывается цель обработки персональных данных)

Даю своё согласие на совершение следующих действий с моими персональными данными (**ненужное зачеркнуть**): сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Даю своё согласие на использование следующих способов обработки моих персональных данных (**ненужное зачеркнуть**):

- с использованием средств автоматизации (автоматизированная обработка);
- без использования средств автоматизации (неавтоматизированная обработка);
- смешанная обработка.

Срок, в течение которого действует согласие: _____

(Указывается срок действия согласия)

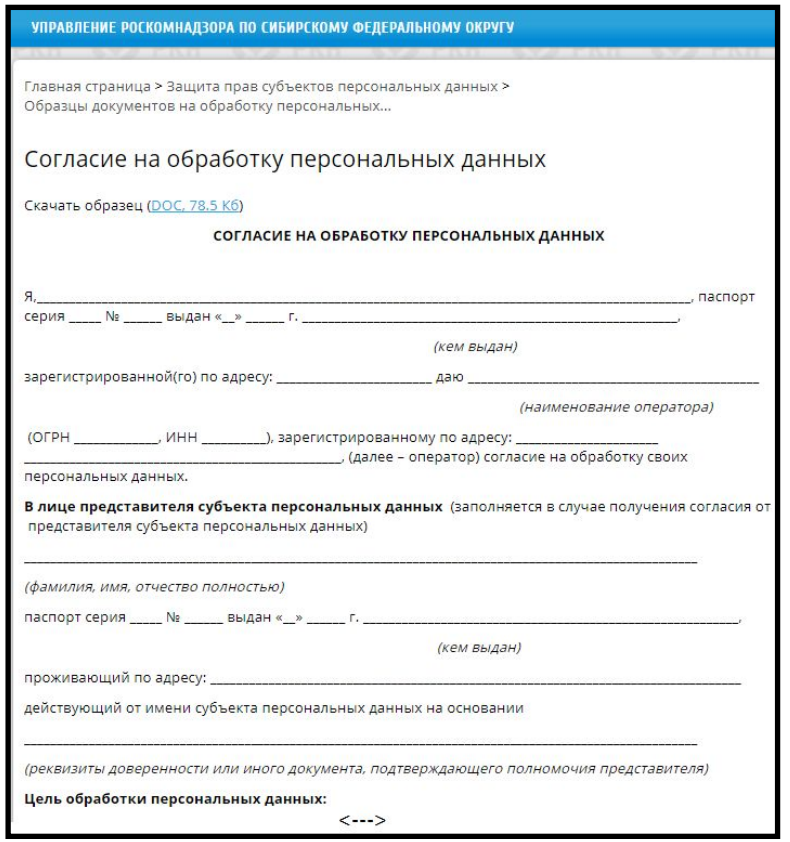
В случае неправомерных действий или бездействия оператора настоящее согласие может быть отозвано мной заявлением в письменном виде.

Дата:

(подпись) (инициалы, фамилия)

Управление Роскомнадзора по Тверской области

https://69.rkn.gov.ru/directions/p1765/p6979/



УПРАВЛЕНИЕ РОСКОМНАДЗОРА ПО СИБИРСКОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ

Главная страница > Защита прав субъектов персональных данных > Образцы документов на обработку персональных...

Согласие на обработку персональных данных

Скачать образец (DOC, 78.5 Кб)

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,_____, паспорт серия _____ № _____ выдан «__» _____ г. _____,

(кем выдан)

зарегистрированной(го) по адресу: _____ даю _____

(наименование оператора)

(ОГРН _____, ИНН _____), зарегистрированному по адресу: _____ _____, (далее – оператор) согласие на обработку своих персональных данных.

В лице представителя субъекта персональных данных (заполняется в случае получения согласия от представителя субъекта персональных данных)

_____

(фамилия, имя, отчество полностью)

паспорт серия _____ № _____ выдан «__» _____ г. _____,

(кем выдан)

проживающий по адресу: _____

действующий от имени субъекта персональных данных на основании

_____

(реквизиты доверенности или иного документа, подтверждающего полномочия представителя)

Цель обработки персональных данных:

<--->

Управление Роскомнадзора по Сибирскому федеральному округу

https://54.rkn.gov.ru/protection/docsamples/

Согласие на обработку ПДн в электронной форме

ч.4. Ст. 9 Федерального закона от 27.07.2017 г. № 152-ФЗ

Согласие в форме электронного документа, подписанного электронной подписью субъекта ПДн признается равнозначным письменному согласию, содержащему собственноручную подпись субъекта ПДн

Управление Роскомнадзора по Смоленской области

Вопрос: Возможно ли получение согласия на обработку персональных данных по телефону? Что является доказательством получения согласия на обработку персональных данных при покупке товаров в интернет-магазинах?

Ответ: При заполнении вэб-формы заявки на покупку товара на сайте интернет-магазина в информационно-телекоммуникационной сети «Интернет» критерием, свидетельствующим о получении оператором согласия субъекта персональных данных на обработку его персональных данных является файл электронной цифровой подписи.

Кроме того, предложения оператора о продаже товара в отдельных случаях может рассматриваться как публичная оферта.

Таким образом, субъект персональных данных, акцентируя указанную оферту, тем самым осуществляет конклюдентные действия, выражающие его волю и согласие на обработку его персональных данных, предоставленных при заполнении заявки на покупку товаров.

Получение согласия на обработку персональных данных по телефону, посредством СМС-сообщений действующим законодательством Российской Федерации не установлено.

Невыполнение оператором обязанности по обеспечению доступа к политике обработки ПДн

Политика не размещена на официальном сайте или информационном стенде (в тех случаях, когда ПДн субъектов не поступают из сети интернет)

В соответствии с Рекомендациями Роскомнадзора, опубликованными на официальном сайте 27.07.2017 г. в «Политику» рекомендуется включить следующие структурные компоненты:

- ✔ *Общие положения (назначение документа, основные понятия, основные права и обязанности оператора и субъекта (ов) персональных данных);*
- ✔ *Цели сбора персональных данных;*
- ✔ *Правовые основания обработки персональных данных;*
- ✔ *Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных;*
- ✔ *Порядок и условия обработки персональных данных (перечень действий, используемые способы и сроки обработки персональных данных);*
- ✔ *Сведения о принятии мер, предусмотренных ч. 2 ст. 18.1, ч. 1 ст. 19 ФЗ от 27.07.2006 № 152;*
- ✔ *Условия прекращения обработки персональных данных.*

ч.3. Ст. 13.11.

Невыполнение оператором обязанности по предоставлению частному лицу информации об обработке его ПДн

Порядок запроса субъектом информации об обработке его ПДн описан в ст. 14 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»

Обязанности оператора при обращении к нему субъекта ПДн либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных описан в ст. 20 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных»

- *соответствует ли запрос требованиям п.3 статьи 14 ФЗ от 27.07.2006 № 152-ФЗ (паспортные данные, подтверждение факта обработки ПДн);*
- *предоставить ПДн в доступной форме, не содержащие ПДн других субъектов и в течение 30 дней.*

ч.4. Ст. 13.11.

Невыполнение в установленные сроки требования о блокировании-уничтожении-изменении ПДн

Блокирование и уничтожение ПДн осуществляется в течении 30 дней после получения запроса, оформленного должным образом.

Оператор вправе продолжить обработку или хранение ПДн, даже при поступлении от субъекта письменного запроса на блокирование/уничтожение в целях осуществления и выполнения возложенных законодательством РФ функций, полномочий и обязанностей

- *«Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ*
- *ФЗ РФ от 02.05.2006 г. № 59 «О порядке рассмотрения обращений граждан Российской Федерации»*

Сроки хранения материальных носителей таких ПДн определены в «Перечне типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», утвержденном Приказом Минкультуры России от 25.08.2010 N 558

ч.5. Ст. 13.11.

Невыполнение обязанностей по хранению материальных носителей ПДн

Постановление Правительства РФ от 15 сентября 2008 г. N 687

- *п. 13. В отношении каждой категории персональных данных необходимо определить **места хранения ПДн** (материальных носителей) и установить **перечень лиц**, осуществляющих обработку ПДн либо **имеющих к ним доступ**;*
- *п. 14. **Раздельное хранение ПДн** (материальных носителей), обработка которых осуществляется в различных целях.*
- *п. 15. При хранении материальных носителей должны соблюдаться условия, **обеспечивающие сохранность** ПДн и **исключающие несанкционированный к ним доступ**. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, **устанавливаются оператором**.*

Федеральный закон от 27.07.2006 N 152-ФЗ

- *п.5. ч.2. Ст.19. Учет машинных носителей*

ч.6. Ст. 13.11.

Невыполнение обязанностей по хранению материальных носителей ПДн

- *Перечень мест хранения ПДн;*
- *Перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;*
- *Журнал учета машинных носителей;*
- *Регламент работ с материальными носителями ПДн:*
  - *Требования к учету машинных носителей (кто ведет учет, в какой форме);*
  - *Правила работы с бумажными носителями:*
    - *хранение только в специально отведенных местах (запираемых шкафах, сейфах);*
    - *раздельное хранение носителей ПДн (в зависимости от целей и допущенных лиц);*
    - *обязанности работников, допущенных к работе с носителями ПДн (покидая рабочее место, убрать носители ПДн в хранилище, либо при отсутствии иных работников, допущенных в помещение, запереть и опечатать дверь).*

ч.6. Ст. 13.11.

Невыполнение обязанности по обезличиванию ПДн либо несоблюдение установленных требований или методов

Обязанность обезличивания ПДн

- *информация, содержит ПДн, но является частью проведенного исследования (в том числе статистического), с последующей публикацией результатов;*
- *информация, содержит ПДн, но подлежит обязательной публикации в СМИ;*
  - *сведения о доходах, расходах, об имуществе и обязательствах имущественного характера государственных служащих и членов их семей (публикация не всех сведений).*
  - *публикование судебных актов (из ПДн в акте остаются только фамилия и инициалы участников судебного дела, остальные сведения исключаются из открытого доступа, такие как адреса, марки автомобилей и т.п.)*

ч.7. Ст. 13.11.

Невыполнение обязанности по обезличиванию ПДн либо несоблюдение установленных требований или методов

Постановление Правительства РФ от 6 сентября 2014 г. № 911 « внесении изменений…»

Постановление Правительства РФ от 6 сентября 2014 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ № 152…»

- *правила работы с обезличенными данными и описание применяемых мер обезличивания в соответствии с «Требованиями и методами по обезличиванию ПДн», утвержденными Приказом Роскомнадзора от 5 сентября 2013 г. № 996*
- *перечень должностей, ответственных за обезличивание*

ч.7. Ст. 13.11.

«Контроль и надзор»

Органы, уполномоченные осуществлять контроль и надзор в сфере обработки ПДн

ФСБ России

Контроль и надзор за выполнением требований к обеспечению безопасности ПДн при их обработке в ИСПДн, в том числе ***с использованием СКЗИ***

- ✔ *ПП РФ от 01.11.2012 г. № 1119*
- ✔ *Приказы ФСБ России:*
  - *от 10.07.2014 г. № 378*
  - *от 09.20.2005 г. № 66*
- ✔ *Приказ ФАПСИ от 13.06.2001 г. № 152*
- ✔ *Методические рекомендации ФСБ 149/7/2/6-432 от 31.03.2015*

Роскомнадзор

Контроль и надзор за соответствием обработки ПДн требованиям законодательства:

- ✔ *Федеральные Законы РФ:*
  - *от 27.07.2006 г. № 152*
  - *от 02.05.2006 г. № 59*
- ✔ *ПП РФ:*
  - *от 21.03.2012 г. № 211*
  - *от 15.09.2008 г. № 687*

ФСТЭК России

Контроль и надзор за выполнением требований к обеспечению безопасности ПДн при их обработке в ИСПДн, ***без использования СКЗИ***

- ✔ *Приказ ФСТЭК России от 18.02.2013 г. № 21*

Вы имеете право

Федеральный закон Российской Федерации от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля»

Плановые

Внеплановые

Проверки

Документарные

Выездные

Вы имеете право

Глава 3. Федеральный закон Российской Федерации от 26 декабря 2008 г. № 294-ФЗ

Руководитель, иное должностное лицо или уполномоченный представитель юридического лица непосредственно присутствовать при проведении проверки, давать объяснения по вопросам, относящимся к предмету проверки

Ознакомиться с результатами проверки, указать в акте проверки свое согласие или несогласие с ними, а также с отдельными действия должностных лиц органа осуществляющего контроль

Обжаловать действия (бездействие) должностных лиц органа государственного контроля (надзора), органа муниципального контроля, повлекшие за собой нарушение прав юридического лица, при проведении проверки, в административном и (или) судебном порядке

Федеральная служба безопасности Российской Федерации

Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Утвержденный Руководством 8 Центра ФСБ России 08 августа 2009 года № 149/7/2/6-1173

Что необходимо знать

При проведении проверки должностные лица 8 Центра ФСБ России не вправе:

проверять выполнение требований, не относящихся к компетенции ФСБ России

требовать представления документов, информации, если они не являются объектами проверки и не относятся к предмету проверки, а также изымать оригиналы документов, относящихся к предмету проверки

Какие документы могут быть запрошены?

Ведомственные документы и приказы по организации криптографической защиты информации	*- положение об обращении с СКЗИ;* *- инструкция пользователя СКЗИ;* *- инструкция ответственного за обращение с СКЗИ;* *- регламент обучения сотрудников правилам работы с СКЗИ;* *- приказы, утверждающие вышеуказанные документы.*
Модель угроз	*- модель угроз*
Документы по поставке СКЗИ оператору. Акты ввода СКЗИ в эксплуатацию	*- акты приема / передачи СКЗИ;* *- договор на закупку /поставку СКЗИ;* *- акты установки СКЗИ на рабочие места пользователей.*
Документация на СКЗИ	*- лицензия на каждое СКЗИ (поставляется в комплекте);* *- сертификаты (в открытом доступе, на сайте поставщика);* *- документация по использованию и установке (в открытом доступе, на сайте поставщика).*

Какие документы могут быть запрошены?

Утвержденный список лиц, допущенных к работе с СКЗИ. Документы, подтверждающие функциональные обязанности сотрудников. Документы, подтверждающие прохождение обучения сотрудников.	- *список лиц, с установленными или выданными СКЗИ;* - *акт / заключение о готовности пользователя к самостоятельной работе с СКЗИ;* - *должностные обязанности сотрудников.*
Журналы СКЗИ	- *журнал учета СКЗИ (как программных, так и аппаратных), с указанием пользователей, которым они выданы*
Дистрибутивы СКЗИ	- *дистрибутивы СКЗИ*
Помещения, выделенные для установки СКЗИ и хранения ключевых документов к ним.	- *перечень помещений с установленными СКЗИ;* - *перечень мест хранения СКЗИ (сейфов).*

Что необходимо знать

При проведении проверки должностные лица 8 Центра ФСБ России не вправе:

превышать установленные сроки проведения проверки

осуществлять плановую или внеплановую проверку в случае отсутствия при ее проведении руководителя или уполномоченного представителя юридического лица, индивидуального предпринимателя, его уполномоченного представителя

Что необходимо знать

При проведении проверки должностные лица 8 Центра ФСБ России не вправе:

осуществлять выдачу предписаний или предложений о проведении мероприятий по контролю за счет проверяемой организации

распространять информацию, составляющую охраняемую законом тайну и полученную в результате проведения проверок, за исключением случаев, предусмотренных законодательством РФ

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций

Административный регламент *предоставления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного контроля (надзора) за соблюдением обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных* ***утвержден Приказом Министерства связи и массовых коммуникаций Российской Федерации от 14.11.2011 № 312***

Перечень запрашиваемых документов

Копии документов, которые рекомендуется подготовить заранее:

1. *Договор с организацией - представителем интересов оператора в ходе проверки;*
2. *Учредительные документы оператора (Устав, свидетельства: ИНН, ОГРН, внесение в ЕГРЮЛ и выписка из него);*
3. *Договор об аренде или праве собственности (помещения, здания занимаемые организацией);*
4. *Уведомление об обработке ПДн;*
5. *Обезличенные согласия субъектов на обработку ПДн;*
6. *Письменные согласия субъектов на обработку ПДн ;*
7. *Приказ о назначении ответственного лица;*
8. *Должностные регламенты работников, допущенных к обработке ПДн;*
9. *Приказ об утверждении Положения о порядке обработки ПДн;*
10. *Положение о порядке обработки ПДн;*
11. *Политика обработки ПДн;*
12. *Иные локальные документы Оператора по защите ПДн (регламенты, инструкции, положения, приказы).*

Копии документов, которые необходимо подготовить непосредственно перед проверкой:

1. *Журналы учета обращений граждан;*
2. *Журналы обращений субъектов ПДн;*
3. *Журналы, реестры, книги, содержащие ПДн;*
4. *Журналы, реестры, книги содержащие ПДн, необходимые для однократного пропуска в здание или на территорию, или в аналогичных целях;*
5. *Перечень лиц допущенных к обработке ПДн;*
6. *План внутренних проверок состояния системы защиты информации;*
7. *Приказ о закреплении помещений, выделенных для обработки ПДн, с приложением перечня лиц, имеющих допуск в помещения (наименования помещений, их номера);*
8. *Приказ об утверждении мест хранения материальных носителей ПДн;*
9. *Типовые формы документов, предполагающие или допускающие содержание персональных данных (перечни, журналы, анкеты, запросы, ответы на запросы и т.п.);*
10. *Распечатки электронных шаблонов полей, содержащих ПДн (Скриншоты таблиц ИСПДн, с удаленными ПДн);*
11. *Договора оператора с третьими лицами на обработку ПДн (поручение оператора);*
12. *Акты об уничтожении ПДн.*

Копии специфических документов:

1. *Документы, подтверждающие соблюдение требований законодательства РФ при обработке специальных категорий и биометрических ПДн;*
2. *Копия обезличенного согласия на обработку ПДн специальных категорий;*
3. *Копия положения о подразделении, осуществляющем функции по организации защиты ПДн;*
4. *Копия Положения о подразделении, осуществляющем функции по организации защиты ПДн;*
5. *Копии лицензий на виды деятельности, в рамках которых осуществляется обработка ПДн;*
6. *Согласие на трансграничную передачу ПДн.*

Основные нарушения в сфере обработки ПДн, регулярно отражаемые в Предписаниях Роскомнадзора

Неверно заполненное уведомление о намерении осуществлять обработку ПДн

Информация, указанная в пункте «Правовое основание обработки ПДн» не подтверждает законность осуществления оператором сбора ПДн

Необходимо указывать, на основании чего осуществляется сбор ПДн, по каждой из целей, преследуемых Оператором:

Цель:	*Правовое основание:*
Прием обращений граждан, подготовка ответов	*Федеральный закон от 02.05.2006 г. № 59 «О порядке рассмотрения обращений граждан РФ»*
Осуществление кадровой работы, начисление заработной платы	*«Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ*
Предоставление государственной услуги по выдаче архивных справок	*Федеральный закон от 22.10.2004 №125-ФЗ "Об архивном деле в Российской Федерации"*

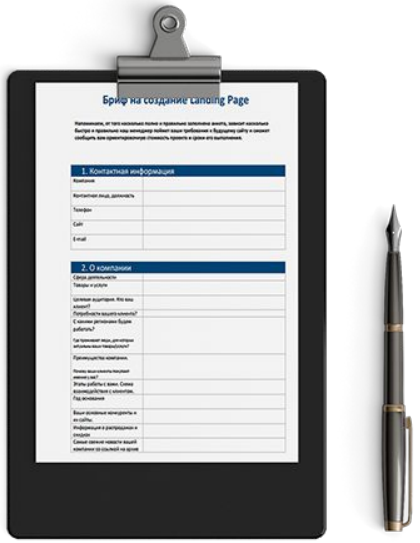
Неверно заполненное уведомление о намерении осуществлять обработку ПДн

- *В уведомлении указаны не все цели, для достижения которых осуществляется сбор ПДн;*
- *В уведомлении указаны не все категории субъектов ПДн;*
- *Сведения об информационных системах заполняются не в полном объеме, необходимо указать все данные для каждой из информационных систем. Количество информационных систем приравнивается к количеству субъектов ПДн.*

Не внесены изменения в уведомление о намерении осуществлять обработку ПДн

Работники, допущенные к обработке ПДн не ознакомлены с локальными документами организации, регламентирующими правила обработки ПДн

Один лист ознакомления со всеми организационно-распорядительными документами, регламентирующими правила работы с ПДн в организации (регламенты, инструкции, положения, политики), подшитый в личное дело работника, допущенного к обработке ПДн



Согласие на обработку ПДн не соответствует требованиям, описанным в ч.4. ст.9 ФЗ № 152

Утвердить в организации формы, предлагаемые Роскомнадзором

РОСКОМНАДЗОР

В организациях берут согласие на обработку всех ПДн субъекта с указанием общего перечня ПДн и всех целей обработки

Данное действие нарушает ч.7. ст. 5. Федерального закона № 152, а именно обязанность уничтожения или обезличивания ПДн при достижении заранее установленной цели. Если таких целей указано несколько, то по достижению хоть одной из них оператор не имеет права продолжить обработку ПДн и все полученные от субъекта ПДн должны быть уничтожены.

В организациях берут согласие на обработку всех ПДн субъекта, с указанием общего перечня ПДн и всех целей обработки

Также это нарушает право субъекта ПДн отозвать согласие на обработку ПДн, если одна из целей обработки утратила актуальность (например, отпала необходимость в получении информации посредством СМС-сообщений на номер мобильного телефона субъекта), но для достижения оставшихся целей (участие в акции, проходящей в настоящий момент) требуется обработка ФИО и данных документа удостоверяющего личность

Нарушение прав субъекта ПДн зачастую приводит к внеплановым проверкам

Отсутствие регламентов уничтожения материальных носителей ПДн и актов об их уничтожении

Разработать локальный документ, регламентирующий порядок уничтожения материальных носителей ПДн, включающий в себя:

- *сроки хранения всех категорий материальных носителей ПДн (личные дела работников, анкеты, резюме и т.п.);*
- *способы уничтожения;*
- *форма акта об уничтожении.*

Отсутствие договоров со сторонними организациями, в которые осуществляется передача ПДн субъектов. Нарушения порядка передачи ПДн таким организациям

ч.3. ст.6. Федерального Закона от 27.07.2006 г. № 152
Поручение оператора – договор, контракт с организацией при передаче в обязательном порядке включающий в себя:

- *перечень действий (операций) с ПДн, которые будут совершаться организацией, которой поручается обработка;*
- *цели обработки;*
- *обязанность соблюдения конфиденциальности ПДн;*
- *обязанность обеспечения безопасности ПДн.*

Не проводятся плановые проверки (Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн нормативным правовым актам в области защиты ПДн (п.4. ч.1. ст. 18.1 ФЗ № 152 и п.16 ПП № 211)

Мероприятие	Результат	Примечание
Проверка наличия и состояния ОРД по защите ПДн		
Проверка наличия и состояния ОРД по обращению с СКЗИ		
Актуализация списков и перечней		
Проверка наличия согласий на обработку ПДн субъектов		
Проверка наличия подписанных обязательств о неразглашении		
Проверка наличия подписей всех работников, допущенных к обработке ПДн в листе(ах) ознакомления.		
Проверка наличия актов об установке СКЗИ		
Проверка актуальности записей, приведенных в журналах		

Списки и перечни находятся в неактуальном состоянии

Оценка эффективности принимаемых мер защиты информации, в соответствии с Приказом ФСТЭК России от 18.02.2013 г. № 21

Самостоятельно

С привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации

В состав мер по обеспечению безопасности персональных данных входят:

1. *идентификация и аутентификация субъектов доступа и объектов доступа;*
2. *управление доступом субъектов доступа к объектам доступа;*
3. *ограничение программной среды;*
4. *защита машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн;*
5. *регистрация событий безопасности;*
6. *антивирусная защита;*
7. *обнаружение (предотвращение) вторжений;*
8. *контроль (анализ) защищенности ПДн;*
9. *обеспечение целостности информационной системы и ПДн;*
10. *обеспечение доступности ПДн;*
11. *защита среды виртуализации;*
12. *защита технических средств;*
13. *защита информационной системы, ее средств, систем связи и передачи данных;*
14. *выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности ПДн, и реагирование на них;*
15. *управление конфигурацией информационной системы и системы защиты ПДн.*

II. Управление доступом субъектов доступа к объектам доступа

	II. Управление доступом субъектов доступа к объектам доступа (УПД)
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники

В общем необходимо рассмотреть 109 мер с указанием методов их реализации в организации (в случае актуальности)

Заключение - рекомендации

- ✔ *В обязательном порядке и в первую очередь обратить внимание на то, выполняются ли в вашей организации те требования законодательства в сфере обработки ПДн, за нарушение которых предусмотрена административная ответственность в соответствии со статьей 13.11 КоАП РФ;*
- ✔ *Ознакомиться с положениями ФЗ РФ от 26.12.2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» и регламентами органов, осуществляющих контроль и надзор в области защиты ПДн;*
- ✔ *Ознакомиться с графиком осуществления плановых проверок, на сайтах: Управления Роскомнадзора по РК (https://11.rkn.gov.ru), ФСБ России (http://fsb.ru), ФСТЭК России (http://fstek.ru).*
- ✔ *Подготовить заранее копии организационно-распорядительных документов (учредительные документы, приказы, положения, инструкции регламентирующие обработку ПДн, должностные инструкции), которые могут быть запрошены в рамках документарной или выездной проверки, и которые не претерпевают изменений с течением времени.*
- ✔ *Если ваша организация внесена в план проверок и вы понимаете, что уровень подготовки к проверке минимален, а уровень понимания данного процесса сильно ограничен - обратитесь за помощью к организации, обладающей соответствующими лицензиями и опытом работы с подобного рода мероприятиями.*

Спасибо за внимание

8 (8212) 301 204 – Отдел продаж ГАУ РК «ЦИТ»

Сыктывкар, 2017 г.