Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Иркутской области

«Регулирования деятельности операторов в области обработки персональных данных.

г. Иркутск

2010 г.

Контактная информация

Адрес Управления Роскомнадзора по Иркутской области

664011, г. Иркутск, ул. Халтурина, д. 7, а/я 169

Сайты

38.rsoc.ru / 38.роскомнадзор.рф
rsoc.ru / роскомнадзор.рф
pd.rsoc.ru

Телефоны/факс

8 (3952) 25-50-93, 34-19-91
28-91-69, 28-91-53,
28-91-63

Отдел по защите прав субъектов персональных данных и надзора в сфере информационных технологий

Начальник отдела:
Савченко Александр Леонидович;
Главный специалист – эксперт:
Лавров Алексей Геннадьевич;
Ведущий специалист – эксперт:
Дворницкая Анна Алексеевна;
Специалист 1 разряда:
Сапрыкина Олеся Васильевна.

Нормативные правовые акты, регулирующие деятельность в области персональных данных.

- Конституция Российской Федерации (ст. 23,24);
- Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ (Глава 14 – «Защита персональных данных работника»;
- Федеральный закон от 27.07.2004 N 79-ФЗ (ред. от 29.01.2010) "О государственной гражданской службе Российской Федерации" (принят ГД ФС РФ 07.07.2004) (ст. 42)
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»;
- Федеральный закон от 10.01.2003 № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации «Выборы»;
- Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» и т.д.

Нормативные правовые (специальные) акты, регулирующие деятельность в области персональных данных.

- Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.);
- Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных»;
- Постановление Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» ;
- Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;
- Приказ Роскомнадзора от 16 июля 2010 г. № 482 "Об утверждении образца формы уведомления об обработке персональных данных"

Нормативные правовые акты, устанавливающие требования по обеспечению безопасности при обработке персональных данных

- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»
- Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах защиты информации в информационных системах персональных данных»;
- Методические документы ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- Методические документы ФСТЭК России. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации утв. Руководством 8 Центра ФСБ РФ от 21.02.2008 № 149/54-144;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных утв. Руководством 8 Центра ФСБ РФ от 21.02.2008 № 149/6/6-622.

Государственное регулирование в области обработки персональных данных

Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных» определяет федеральные государственные органы (регуляторы) по регулированию, осуществлению контроля и надзора в области соблюдения требований вышеуказанного закона операторами

ч. 3 ст. 19

ФСТЭК России, федеральный орган уполномоченный в области

ПД ИТР и ТЗИ

ФСБ России, федеральный орган, уполномоченный в области

обеспечения безопасности

ч. 1 ст. 23

Роскомнадзор

уполномоченным органом по защите **прав субъектов персональных данных**

(Постановление Правительства от 16.03.2009 г. № 228)

Нормативные документы ФСТЭК России

Нормативные документы ФСБ России

Административный регламент о проведении проверок (Приказ от 01.12.2009 г. № 630)

Административный регламент о ведении реестра операторов (Приказ от 30.01.2010 г. № 18)

Основные положения Федерального Закона от 27.07.06г. №152-ФЗ «О персональных данных

Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных

Способы обработки Персональных данных

Использование персональных данных - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Основные положения Федерального Закона от 27.07.06г. №152-ФЗ «О персональных данных

Оператор (ст. 3)

государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

Федеральные органы государственной власти	Центральные аппараты, территориальные органы федеральных органов исполнительной власти
Исполнительные органы государственной власти субъектов РФ	Правительства и Администрации субъектов РФ, их структурные подразделения
Государственные органы	ГУПы, в т.ч. Центры занятости населения
Органы местного самоуправления	ОМСУ всех уровней
Муниципальные органы	Больницы, детские сады, коммунальные службы и др.

Юридические, физические лица, осуществляющие обработку ПДн с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации.

Согласие субъекта персональных данных на обработку своих персональных данных ст. 9

Субъект персональных данных принимает решение о предоставлении своих персональных данных и дает согласие на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных законом

Федеральными законами предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства

Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных лежит на операторе

Для обработки персональных данных, содержащихся в согласии в письменной форме субъекта на обработку его персональных данных, дополнительного согласия не требуется

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

Письменное согласие субъекта персональных данных на обработку своих персональных данных должно включать в себя:

фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе

перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных

цель обработки персональных данных

перечень персональных данных, на обработку которых дается согласие субъекта персональных данных

наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных

срок, в течение которого действует согласие, а также порядок его отзыва.

Конфиденциальность персональных данных ст. 7

обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания

Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных

Меры по охране конфиденциальности персональных данных, принимаемые оператором, должны включать в себя:

- определение перечня персональных данных, переданных оператору для обработки и включенных в число сведений конфиденциального характера;
- ограничение доступа к персональным данным путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к обрабатываемым персональным данным, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию персональных данных работниками оператора на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- применение мер технической защиты информации.

Меры по охране конфиденциальности персональных данных, понимаются разумно достаточными, когда

- исключается доступ к обрабатываемым персональным данным любых лиц без согласия их обладателя;
- обеспечивается возможность использования обрабатываемых персональных данных работниками оператора и передачи ее контрагентам без нарушения установленного режима защиты.

Обязанности оператора

Перед уполномоченным органом

1. Направить уведомление об обработке персональных данных в уполномоченный орган и иные действия. связанные с ведение государственного реестра операторов ст. 22
2. Выполнить требования уполномоченного органа в т.ч. предоставить запрашиваемую им информацию в порядке, предусмотренном законом ст. 9, ст. 20, ст. 21, ст. 23

Перед субъектом ПД

1. Предоставить субъекту ПД установленную законом информацию ст. 9, ст. 14. ст. 18. ст. 20
2. Устранить нарушения законодательства, допущенные при обработке ПД, а также по уточнению, блокированию и уничтожению ПД

При обработке ПД, принимать необходимые организационные и технические меры для защиты ПД

Принятие решения, порядок подготовки и направление уведомления

Каждому оператору ПД (государственному или муниципальному органу, юридическому или физическому лицу, организующему и (или) осуществляющему обработку ПД, а также определяющему цели и содержание обработки ПД) перед началом обработки ПД необходимо ознакомиться с законодательством в области обработки персональных данных

Принять решение в соответствии с требованиями ст. 22 152-ФЗ о предоставлении Уведомления об обработке персональных данных в уполномоченный орган по защите прав субъектов ПД

В случае принятия решения о подачи уведомления в уполномоченный орган по защите прав субъектов ПД провести все необходимые мероприятия, по Регистрации в качестве оператора обрабатывающего ПД, и дальнейшей работы, предусмотренной, действующим законодательством по внесению изменений в т.ч. исключение из реестра операторов обрабатывающих ПД

Работа с уведомлением

Начало обработки ПД → **Уведомить уполномоченный орган по защите прав субъектов ПД о своем намерении осуществлять обработку ПД**

ч. 1 ст. 22

Уведомление → **направляется в письменной форме,** в т.ч. при помощи электронного портала «Персональные данные» подписанное уполномоченным лицом **или** направляется в электронной форме и **подписано электронной цифровой подписью** в соответствии с законодательством РФ.

ч. 3 ст. 22

В случае требования уполномоченного органа по защите прав субъектов персональных данных предоставить уточненные сведения.

ч. 6 ст. 22

Уведомить об изменениях уполномоченный орган по защите прав субъектов ПД в течение ***десяти рабочих дней*** с даты возникновения таких изменений.

п. 7 ст. 22

Мероприятия, проводимые оператором после подачи уведомления

При обработке персональных неавтоматизированным способом:

- Обеспечить при обработке ПД требования, предусмотренные п.п. 3, 5, 6, 7,8, 13, 15 Постановления Правительства РФ от 15 сентября 2008 г. № 687;
- Разработать документ (положение, правила), регламентирующий правила обработки персональных данных, осуществляемых без использования средств автоматизации;
- Утвердить приказом (распоряжением)перечень (списки) лиц, обрабатывающих персональные данные;
- Ознакомить под роспись всех сотрудников с нормативными, локальными документами, регламентирующими обработку ПД в организации;
- Подготовить документы и провести все необходимые мероприятия, обеспечивающие соблюдение требований ст. 86-90 ТК; ст. 6, 9, 10, 11, 22 Федерального закона 152-ФЗ.

При обработке персональных автоматизированным способом:

- Организовать работу и Обеспечить при обработке ПД требования, Постановления Правительства РФ Постановление Правительства Российской Федерации от 17.11.2007 №781
- Разработать документ (положение, правила), регламентирующий правила обработки персональных данных, осуществляемых с использованием средств автоматизации;
- Утвердить приказом (распоряжением)перечень (списки) лиц, обрабатывающих персональные данные;
- Ознакомить под роспись всех сотрудников с нормативными, локальными документами, регламентирующими обработку ПД в организации;
- Выявить все свои ИСПД;
- Привести в соответствии с требованиями до 01.01.2011 г.;
- Определить назначение ИСПД и круг лиц, работающих с данной ИСПД, описать все это документально;
- Классифицировать все свои ИСПД;
- Создать модель угроз для каждой конкретной ИСПДН, описать средства защиты, разработать ряд нормативных документов;
- Обеспечить техническими и организационными мерами требуемый уровень безопасности для каждой конкретной ИСПД в соответствии с ее классом.

При смешанной обработке персональных данных провести мероприятия, предусмотренные обоими случаями

Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Иркутской области

Спасибо за внимание

Начальник отдела по защите прав субъектов персональных и правового обеспечения Управления Роскомнадзора по Иркутской области – Савченко Александр Леонидович