



Введение

Начнем с того, что такое персональные данные и где они присутствуют? Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В персональные данные входит имя, место проживания и другая информация. Каждая компания обладает информацией о своих работниках, вносит эти данные в документацию и хранит их. Когда компания принимает на работу нового сотрудника или заключает договор с клиентом – физическим лицом, она получает данные человека: его имя и фамилию, адрес, и т. п. В персональные данные входит много различной информации, также есть правила работы с ней. Если компания их нарушит, контролеры назначат крупный штраф. С 1 июля 2017 года действуют новые правила привлечения к административной ответственности за подобные нарушения. Для решения подобных вопросов существует специальный государственный орган или это может быть физическое лицо – оператор. 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.

Законы о защите персональных данных

Правоотношения в сфере персональных данных регулируются федеральным законодательством РФ (Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»), Трудовым кодексом РФ (глава 14), а также Гражданским кодексом РФ.

Основные положения Закона «О персональных данных»

- Обработка персональных данных должна осуществляться на законной и справедливой основе, в строгом соответствии с установленными целями обработки персональных данных.

- Недопустимо раскрытие персональных данных третьим лицам или распространение таких данных без соответствующего основания (согласия субъекта либо требований федеральных законов).
- В ряде случаев обработка персональных данных может осуществляться только с согласия субъекта персональных данных.
- Информационные системы, обрабатывающие персональные данные, должны быть приведены в соответствие с требованиями законодательства о персональных данных.
- Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда, обжаловав действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- Оператор обязан направить уведомление об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных. Таким органом является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (более известная как Роскомнадзор);
- Нарушение требований Закона влечет гражданскую, уголовную, административную, дисциплинарную ответственность.

Методы защиты персональных данных

Защита персональных данных осуществляется с помощью комплекса действий:

Организационные меры по защите персональных данных включают в себя:

- Назначение лиц, ответственных за организацию обработки и обеспечение безопасности персональных данных;
- Разработку организационно-распорядительных документов, регламентирующих весь процесс получения, обработки, хранения, передачи и защиты персональных данных;
- Внесение изменений в бизнес-процессы организации, ознакомление пользователей, осуществляющих обработку персональных данных с положениями нормативных документов;
- Заключение дополнительных соглашений с контрагентами и третьими лицами, которым передаются персональные данные либо поручается их обработка;
- Определение перечня мероприятий по защите персональных данных и реализация таких мероприятий;

- Осуществление внутреннего контроля соответствия обработки и защиты персональных данных требованиям законодательства.

Технические меры по защите персональных данных предполагают внедрение и использование программно - аппаратных средств защиты информации. При осуществлении обработки ПДн с использованием средств автоматизации, применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется исходя из уровня защищенности системы персональных данных.

Требования к информационным системам персональных данных

Определение уровня защищенности информационных систем персональных данных производится операторами самостоятельно в зависимости от объема и категории обрабатываемых персональных данных, а также типа актуальных угроз в соответствии с Постановлением Правительства № 1119 от 01.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Данное Постановление Правительства также определяет требования по обеспечению безопасности персональных данных при их обработке в информационных системах в соответствии с их уровнем защищенности.

Помимо этого, детализированные требования по защите персональных данных установлены, в частности:

- приказом ФСТЭК № 21 от 18.02.2013 г;
- приказом ФСБ № 378 от 18.08.2014 г. (в случае необходимости применения для защиты персональных данных шифровальных (криптографических) средств защиты информации).

Также, согласно требованиям новой редакции Федерального закона №152-ФЗ «О персональных данных» с изменениями, внесенными Федеральным законом от 21.07.2014 г. №242-ФЗ и Федеральным законом от 31.12.2014 г. №526-ФЗ, базы данных информационных систем, в которых осуществляется запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации должны быть расположены на территории РФ.

Контроль

Контроль за выполнением законодательства возложен на следующие органы:

- Уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) – основной надзорный орган в области персональных данных;
- ФСБ – основной надзорный орган в части использования средств шифрования;
- ФСТЭК – надзорный орган в части использования технических средств защиты информации.

Уполномоченный орган по защите прав субъектов персональных данных проводит как плановые и внеплановые мероприятия по контролю (надзору) за соответствием обработки персональных данных требованиям законодательства Российской Федерации.

Заключение

Подведем итоги преимущества защиты персональных данных. Помимо того, что за нарушение данной защиты идет ответственность на федеральном уровне, защита информации о себе даст дополнительные преимущества:

- Защиту от претензий и штрафов со стороны регулирующих органов;
- Преимущества перед конкурентами, т.к декларирование соответствия требованиям законодательства о персональных данных приведет к повышению прозрачности и доверия к компании со стороны потенциальных и существующих контрагентов и клиентов;
- Отсутствие негативных отзывов в прессе и СМИ, связанных с неудовлетворительными результатами прохождения проверок регулирующих органов;
- Возможность продолжать свою деятельность, не опасаясь претензий со стороны клиентов и собственных сотрудников;
- Возможность работы с персональными данными не только внутри компании, но и при передаче их сторонним организациям;
- Защиту от непредвиденной и принудительной остановки бизнеса;
- Защиту от недобросовестных конкурентов;
- Информационные системы, соответствующие всем стандартам и требованиям законодательства в области персональных данных.

Список источников

- 1.** <https://ru.wikipedia.org/wiki>
- 2.** <http://www.pointlane.ru/personal/>
- 3.** <https://www.law.ru/article/21683-что-входит-в-персональные-данные-и-их-обработку>