Защита персональных данных – это комплекс мероприятий, позволяющий выполнить требования законодательства РФ, касающиеся обработки, хранению и передачи персональных данных граждан.

Согласно требованию закона о защите персональных данных, оператор персональных данных обязан выполнить ряд организационных и технических мер касающихся процессов обработки 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.

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки 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 так же Гражданским кодексом РФ.
Закон «О персональных данных» обязывает оператора принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.
Появление закона поставило сложную и требующую немедленного решения задачу перед большинством российских компаний. До 1 января 2010 года компании (операторы), обрабатывающие персональные данные в информационных системах, обязаны обеспечить:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;
в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Основные положения Закона «О персональных данных»:

- Информационные системы, обрабатывающие персональные данные и созданные до вступления в силу Закона «О персональных данных» должны быть приведены в соответствие с его требованиями не позднее 1 января 2010 года;

- 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);

- 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;

- Нарушение требований Закона влечет гражданскую, уголовную, административную, дисциплинарную ответственность физических и должностных лиц.

Требования к информационным системам персональных данных

Требования к обеспечению безопасности персональных данных установлены Постановлением Правительства № 781 от 17.11.2007 г. «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных». Положение определяет требования по обеспечению безопасности персональных данных при их обработке

в информационных системах в соответствии с их классом.
Классификация информационных систем производится операторами самостоятельно в зависимости от объема и состава обрабатываемых персональных данных в соответствии с совместным приказом ФСТЭК, ФСБ и Мининформсвязи от 13.02.2008 г. «Об утверждении Порядка проведения классификации информационных систем персональных данных».
Контроль
Контроль за выполнением законодательства возложен на следующие органы:

- 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 производит как плановые и внеплановые мероприятия по контролю (надзору) за соответствием обработки персональных данных требованиям законодательства Российской Федерации. За 2008 год уполномоченный орган произвел 76 плановых проверок и 40 внеплановых, произведенных по в ходе рассмотрения обращений граждан . На 2009 год планируется проведение более 300 плановых проверок.
Комплекс мероприятий по обеспечению защиты персональных данных
Организационные меры по защите персональных данных включают в себя:

- Разработку организационно-распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных;
- Определение перечня мероприятий по защите ПДн.

Технические меры по защите персональных данных предполагают использование программно - аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации, применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется исходя из класса системы персональных данных;
Типичные позиции операторов персональных данных

1. ”Наша компания не собирается ничего предпринимать и тратить время и деньги на решение этих вопросов, мы будем ждать развития событий”.

Такая компания не собирается тратить деньги и время на изменение процессов обработки и хранения персональных данных, а так же не задумывается об обучении своих сотрудников при работе с ними. Организация продолжает свою деятельность в привычном режиме, в надежде на то, что первые компании, которые не выполнят поставленных задач со стороны государственных органов, будут требовать пересмотра и корректировки закона, а так же расширения списка средств, допустимых к использованию в системах защиты ПДн или же сдвинуть сроки готовности системы обработки ПДн.

Ассоциация российских банков (АРБ) уже дважды пыталась безуспешно отсрочить срок приведения информационных систем в соответствие с требованиями ФЗ-152. Сроки выполнения оставлены без изменения.

2. “Мы уверены в том, что действия закона не будут распространяться на нашу компанию”.

В любой компании, вне зависимости от её организационно-правовой формы, есть информация о сотрудниках, работающих в организации, а иногда и её контрагентах. Таким образом такая компания является оператором персональных данных, действия ФЗ-152 распространяются и на неё.

Классическая ситуация: реализовать своими силами, или приглашать консультантов?

Для того чтобы ответить на этот вопрос, необходимо определиться со следующими вещами:

- Готов ли руководитель компании взять на себя ответственность за успешное внедрение средств защиты персональных данных?
- Есть ли у компании квалифицированные сотрудники, которые готовы выполнить требования закона?
- Может ли руководство компании оценить сроки и стоимости такого проекта?
- Как выполнить требования закона по защите персональных данных, при этом не нарушить критические бизнес-процессы компании?
- Каким образом необходимо подавать заявление в регулирующие органы?

Если вышеперечисленные задачи, не могут быть реализованы собственными силами, следует привлекать внешних консультантов.

Компания “Pointlane” оказывает полный цикл услуг по консультационным вопросам, а так же по вопросам прохождения аттестации на работу с персональными данными:

- Консультации по вопросам требований законодательства и определения их действия применительно к Вашей организации;
- Подготовка заявки на регистрацию Вашей организации как оператора персональных данных;
- Инвентаризация персональных данных;
- Построение модели угроз;
- Определение класса ИСПДН (информационных систем персональных данных) и выработка мер по его понижению, тем самым снизив затраты на средства защиты не уменьшая степени защищенности персональных данных;
- Внедрение средств защиты;
- Подготовка ИСПДН к аттестации;
- Подготовка Вашей организации к получению лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации;
- Составление ответов на обращения граждан в рамках законодательства по ПД.

Преимущества проведения мероприятий по защите персональных данных

После внедрения системы по защите персональных данных Заказчик получит:

- 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 претензий со стороны регулирующих органов;

- Защиту от непредвиденной и принудительной остановки бизнеса;
- Защиту от недобросовестных конкурентов;
- Информационную систему соответствующую всем стандартам и требованиям законодательства.