Работа с персональными данными

Анастасия Федорова
Эксперт по информационной безопасности в компании КРОК

Сегодня мы рассмотрим вопросы организации обработки и защиты персональных данных. Сначала ответим на вопрос, для чего же вообще нужно защищать персональные данные.

Что такое «персональные данные» и чем они регулируются?

Если мы откроем новостные сводки, то увидим, что там очень много статей, которые посвящены утечкам личной информации и персональных данных пользователей социальных сетей, сотрудников и работников банков, пользователей банков, а также граждан, которые обращаются в органы государственной власти. Утечки персональных данных затрагивают не только РФ, но и иностранные государства.

На территории РФ в 2006 году был принят Закон «О персональных данных», регулирующий сферу организации обработки и обеспечения безопасности персональных данных. Он также вводит понятие «персональные данные»: «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн)».

Другим участником данной сферы правовых отношений является оператор — лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку ПДн.

Обработка — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн. Выделяются 16 способов обработки персональных данных, в том числе сбор, автоматизация, накопление, хранение, удаление и др.

> Обязанности по обработке и обеспечению безопасности персональных данных возложены на оператора персональных данных. На текущий момент эти обязанности в основном агрегированы в 4 главе Закона «О персональных данных».

Их можно разделить на два больших блока: организационно-процессная часть и техническая часть.

В организационно-процессную часть входит применение необходимых правовых и организационных мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством.

Технические меры связаны с применением необходимых мер по обеспечению безопасности персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий.

Одной из ключевых особенностей при применении организационно-процессных мер является выделение процессов обработки ПДн в бизнес-процессах компании. Необходимо выделить законные и справедливые основы обработки ПДн, конкретные, определенные и законные цели обработки, состав персональных данных, который будет неизбыточен по отношению к заявленным целям. Прекратить обработку данных необходимо в тот момент, когда эти цели будут достигнуты. Либо должны быть другие законные основания для обработки.

Условия обработки ПДн:

- Согласие субъекта ПДн
- Договор, стороной или выгодоприобретателем по которому является субъект ПДн
- Обработка для деятельности журналистов, СМИ, научной, литературной и творческой деятельности в статистических или исследовательских целях
- Обработка ПДн, сделанных субъектом общедоступными, обработка ПДн, сделанных общедоступными на основании законодательства
- Обработка ПДн при судопроизводстве или исполнении судебных актов, исполнении полномочий госорганов, органов местного самоуправления
- Обработка для защиты жизни и здоровья субъекта, если взять согласие невозможно

Согласие субъекта ПДн должно быть:

- Конкретными
- Информированным
- Сознательным
- В любой позволяющей получить факт его получения форме

Особые случаи получения согласий:

- Передача ПДн третьему лицу или поручение обработки
- Включение ПДн в общедоступные источники данных (письменное)
- Обработка специальных категорий ПДн (письменное)
- Обработка биометрических ПДн (письменное)
- Трансграничная передача (письменное)

Письменное согласие субъекта должно содержать:

- ФИО, адрес субъекта ПДн

- Номер основного документа, удостоверяющего личность, сведения о дате выдачи и выдавшем органе
- Наименование и адрес оператора, получающего согласие ПДн
- Цель обработки
- Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных
- Срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва
- Перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных
- Подпись субъекта ПДн
- Наименование или ФИО и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу

Какие дополнительные организационные меры должен выполнить оператор ПДн для приведения своей деятельности в соответствие с требованиями законодательства о персональных данных?

- Уведомление РКН о начале обработки ПДн
- Обработка обращений субъектов ПДн и уполномоченных органов
- Обеспечение конфиденциальности ПДн
- Обеспечение безопасности ПДн при обработке
- Соблюдение требований по локализации БД граждан РФ

Технические меры, направленные на обеспечение безопасности персональных данных:

- Ознакомление работников оператора с правилами обработки и обеспечения безопасности персональных данных и требованиями законодательства об обработке персональных данных
- Проведение регулярных проверок соответствия своей деятельности требованиям законодательства об обработке персональных данных

Общие требования к обеспечению безопасности ПДн:

- Выделение информационных систем персональных данных
- Определение уровней защищенности ПДн
- Нейтрализация актуальных угроз
- Применение системы защиты персональных данных
- Регулярная оценка эффективности принятых мер

Контроль и надзор в данной сфере осуществляет Роскомнадзор, ФСБ, ФСТЭК.

Деятельность РКН в сфере контроля ПДн:

1. Контроль и надзор:
- систематический мониторинг операторов ПДн
- плановые проверки
- внеплановые проверки
2. Ведение реестров:
- операторов ПДн
- нарушителей прав субъектов ПДн
3. Взаимодействие с субъектами ПДн:
- обработка жалоб и обращений субъектов

Таким образом, ключевые обязанности по обеспечению безопасности и обработки ПДн возложены на операторов ПДн. Выполнение обязанностей контролируется Роскомнадзором. Невыполнение обязанностей ведет к административной ответственности. Для выполнения этих обязанностей от организации требуются разработка и поддержание в актуальном состоянии процессов обработки ПДн субъектов, контроль их реализации и внедрения технических средств и мер защиты ПДн, которые также должны проходить регулярный контроль и надзор.