И н ф о р м а ц и я
о положениях законодательства Российской Федерации по вопросам обработки персональных данных.

Вводная часть

Поводом для принятия закона о защите персональных данных является необходимость устранения барьеров в международной торговле со странами Евросоюза. Осуществление обмена персональными данными, зачастую необходимыми при совершении сделок, возможно только между государствами, способными обеспечить соответствующую защиту передаваемой и получаемой информации. Федеральный закон о ратификации Конвенции Совета Европы 1981 года "О защите личности в связи с автоматической обработкой персональных данных". Президент России подписал 19 декабря 2005 года, возложив на Российскую Федерацию обязательства по приведению в соответствие с нормами европейского законодательства деятельность в области защиты прав субъектов персональных данных (далее - СПДн). Первым шагом в реализации взятых обязательств, стало принятие Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных» (далее - Закон) вступившим в силу в январе 2007 года. Данный Закон определил требования к защите персональных данных, которые затем были конкретизированы в подзаконных актах Правительства Российской Федерации и Министерства связи, нормативно - методических документах Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России) и Федеральной службы по надзору в сфере связи и массовых коммуникаций (Роскомнадзор). Каждый из этих актов и документов посвящен отдельным областям и тематикам законодательства в области защиты персональных данных.

Часть 1
Основные понятия

Что же такое персональные данные? К данному термину относят любую информацию, которой достаточно, чтобы однозначно определить физическое лицо и получить о нём какие-либо дополнительные данные. К примеру, если старшая по дому вывесила в подъезде списки должников, в которых указала фамилию, имя отчество ответственного квартиросъемщика, номер квартиры, в которой он проживает и другую информацию, то эти списки являются персональными данными, так как прямо относятся к определенному физическому лицу являющемуся СПДн-ом. А в случае с садоводческим товариществом «Флора», где вывешен график дежурств, с указанием только номера участка и даты дежурства, эта информация персональными данными являться не будет.

Любая организация (называемая в Законе – оператором), работающая с данными физических лиц, должна защитить используемые информационные системы и получить документы, подтверждающие соответствие этих систем требованиям законодательства.

Рассмотрим основные понятия, встречающиеся в данном законе.

Информационными системами персональных данных (далее - ИСПДн) согласно определению в статье 3 Закона называют все содержащиеся в базах данных персональные данные, а так же обеспечивающие их обработку информационные технологии и технические средства.

Термин «обработка персональных данных», в законе определен как: «любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных» иначе говоря все, что мы можем сделать с персональными данными, начиная от их сбора и заканчивая уничтожением, и есть их обработка.

Автоматизированная обработка персональных данных производится с помощью средств вычислительной техники, не автоматизированная – вручную, как правило, она осуществляется в журналах, картотеках, личных делах и на других бумажных носителях.

Передача персональных данных за границу Российской Федерации, на территорию иностранного государства носит название: «трансграничной передачи персональных данных».

Источники персональных данных создаваемые, с целью информирования населения называются общедоступными, они могут быть как электронными, например сайт Университета, так и в бумажном варианте, в виде доски объявлений в холле.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту.

Часть 2
Обязанности оператора

Получение персональных данных в ОмГУПС осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России и Рособразования, локальными нормативными актами.

Законом, установлено, что обработка персональных данных может осуществляться оператором только с согласия субъектов персональных данных, исключение составляют случаи, предусмотренные иными федеральными законами.

Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальности, расовой принадлежности, политических и религиозных убеждениях, его частной жизни.

Персональные данные следует получать у СубъектаПДн. Если персональные данные возможно получить только у третьей стороны, то работник или обучающийся, должен быть уведомлен об этом заранее и от него должно быть получено на это письменное согласие.

Хранение персональных данных должно происходить в порядке, исключающем их утрату или неправомерное использование.

Обработка персональных данных осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия

работникам и студентам в трудоустройстве, обучении, продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы или учебы, обеспечения сохранности имущества.

Персональные данные могут храниться в бумажном и(или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением мер по защите персональных данных. Право на обработку персональных данных предоставляется работникам структурных подразделений и(или) должностным лицам, определенным Положением об обработке и обеспечении безопасности персональных данных, распорядительными документами и иными письменными указаниями.

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Т.е. при поступлении запроса, на предоставление информации содержащей персональные данные она может быть предоставлена только с согласия СПДна, это же относится к трансграничной передаче персональных данных и к общедоступным персональным данным. Данное положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами. Примером, когда получать согласие субъекта персональных данных не требуется, являются мотивированные запросы от органов прокуратуры, правоохранительных органов, органов безопасности, от государственных инспекторов труда при осуществлении ими государственного надзора и контроля, за соблюдением трудового законодательства.

Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

Если в поступившем запросе ставится вопрос о достоверности обучения в ВУЗе, при этом приводится ФИО и атрибуты диплома субъекта персональных данных, то в ответе можно указать следующее: «запрашиваемая Вами информация достоверна /недостоверна». При таком варианте ответа происходит обезличивание персональных данных и соответственно не требуется согласия СПДн-а.

Обработка персональных данных для Фонда социального страхования, Пенсионного фонда, кредитных организаций, открывающих и обслуживающих платежные карты для начисления заработной платы, является обязательной и осуществляется с использованием средств вычислительной техники. Передача этих данных производится только по установленному каналу с применением криптографических средств защиты информации.

Как мы уже отмечали выше, необходимым условием обработки персональных данных является согласие субъекта, поэтому отсутствие этого согласия затрудняет, а иногда и делает невозможным осуществление возложенных на ОмГУПС федеральным законодательством, его уставом функций, полномочий и обязанностей, а также реализацию права на труд, образование, пенсионное обеспечение и медицинское страхование.

Ознакомиться с политикой в отношении обработки персональных данных можно на сайте ОмГУПС, там же находится положение об обработке и обеспечении безопасности персональных данных.

Часть 3
Права субъекта

Субъект ПДн имеет право на свободный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей его персональные данные (за исключением случаев, предусмотренных Законом).

Субъект имеет право отзывать согласие на обработку его персональных данных при этом оператор обязан прекратить их обработку. К примеру, если Вы при оформлении дисконтной карты в магазине «Малахит» предоставили свои персональные данные, а именно сведения об адресе, контактный телефон, ФИО, то на основании статьи 14 закона, написав заявление директору данной торговой точки, Вы можете потребовать прекратить их использование, для распространения любых рекламных сообщений и иных информационных материалов, а также запретить их передачу третьим лицам.

Рассмотрим еще один пример по реализации прав СПДн-а - права требовать от оператора уничтожения его персональных данных. Обратившись в кадровое агентство «Престиж», с целью получения помощи в поиске работы Вы предоставили в их распоряжение следующие персональные данные: ФИО, адрес, сведения об образовании, профессии, о постановке на воинский учет, состоянии здоровья, кроме того при этом проводилась видео и фотосъемка. После приема на постоянную работу нужда в услугах данного агентства была исчерпана, поэтому в соответствии со статьей 21 закона, Вы вправе потребовать удалить всю предоставленную информацию, включая материалы видео и фотосъемки и вернуть оригиналы предоставленных сведений, написав заявление на имя руководителя кадрового агентства.

Как мы видим на приведенных выше примерах, Субъекты свои персональные данные раскрывают зачастую сами, например, оформляя покупку товара с доставкой на дом, регистрируясь на веб-сайте, в социальных сетях. Но далеко не всегда лица, получающие такую информацию, добросовестно сохраняют ее.

Часть 4
Ответственность оператора

Согласно статье 24 Закона лица, виновные в нарушении его требований, несут предусмотренную законодательством Российской Федерации ответственность, в частности: административную (ст. 13.11 "Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)", ст. 5.39 "Отказ в предоставлении информации", ст. 13.14 "Разглашение информации с ограниченным доступом" КоАП РФ), уголовную (ст. 137 "Нарушение неприкосновенности частной жизни", ст. 272 "Неправомерный доступ к компьютерной информации", ст. 140 "Отказ в предоставлении гражданину информации" УК РФ)

При нарушении законодательства Российской Федерации о персональных данных в трудовых отношениях привлечение к дисциплинарной ответственности производится в соответствии со ст. ст. 192, 193, 195 ТК, к материальной ответственности в соответствии со ст. ст. 237, 238, 241 ТК. Также предусмотрена и гражданско-правовая ответственность.

Рассмотрим, какие виды наказания используются при нарушениях законодательства в области защиты персональных данных.

По ст. 5.39 КоАП РФ виновное лицо будет привлечено к ответственности и наказано штрафом в размере от одной тысячи до трех тысяч рублей.

Нарушение по ст. 13.11 КоАП РФ влечет предупреждение или наложение административного штрафа:

- на граждан в размере от 300 до 500 руб.;
- на должностных лиц - от 500 до 1000 руб.;
- на юридических лиц - от 5000 до 10 тыс. руб.

Кроме того, административная ответственность предусмотрена по ст. 13.14 КоАП РФ. В этом случае виновный будет наказан в виде административного штрафа:

- гражданин в размере от 500 до 1000 руб.;
- должностное лицо - от 4000 до 5000 руб.

Закон устанавливает в данной сфере не только административную, но и уголовную ответственность.

По ст. 137 УК РФ виновные лица наказываются:

- штрафом до 200 тыс. руб., либо
- обязательными работами на срок от 120 до 180 часов, либо
- исправительными работами на срок до 1 года, либо
- арестом на срок до 4 месяцев, либо
- лишением свободы на срок до 2 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет.

Если это преступление совершено лицом с использованием своего служебного положения, то наказание будет еще строже.

Должностные лица могут быть привлечены к уголовной ответственности по ст. 140 УК РФ, за что предусмотрено наказание в виде:

- штрафа до 200 тыс. руб., либо
- лишения права занимать определенные должности или заниматься определенной деятельностью на срок от 2 до 5 лет.

Виновные лица по ст. 272 УК РФ несут наказание в виде:

- штрафа до 200 тыс. руб., либо
- исправительных работ на срок до 1 года, либо
- ограничения свободы на срок до 2 лет, либо лишения свободы на тот же срок.

При выявлении корыстной заинтересованности, лица совершившего преступление, наказание усиливается.

В случае разглашения персональных данных работника с сотрудником получившим доступ и разгласившим эти данные, может быть расторгнут трудовой договор по инициативе работодателя в соответствии с подп. "в" п. 6 ч. 1 ст. 81 ТК РФ.

Уполномоченным органом по защите прав СПДн, на который возлагается обеспечение контроля и надзора за соответствием обработки персональных данных требованиям Закона, является - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Уполномоченный орган (называемый в законе – регулятором) рассматривает обращения субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принимает соответствующее решение (ст. 23 Закона).

Роскомнадзор по Омской области по обращению жителя Октябрьского округа г. Омска провел проверку соблюдения закрытым акционерным обществом «Управляющая компания «Партнер-Гарант» требований законодательства о персональных данных.

Установлено, что в нарушение закона данная управляющая компания предоставила третьим лицам копию лицевого счета, содержащую персональные данные жильцов дома, с которыми ранее договор управления был расторгнут.

По итогам проверки в отношении исполнительного директора ЗАО «УК «Партнер-Гарант» было возбуждено дело об административном правонарушении, предусмотренном ст. 13.11 КоАП РФ.

По результатам рассмотрения административного производства должностное лицо, допустившее нарушения, привлечено к ответственности в виде штрафа.

Часть 5
Защита персональных данных

Персональные данные защищаются от несанкционированного доступа в соответствии с Законодательством Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, о которых мы говорили в самом начале, а также локальными актами оператора.

В отношении персональных данных субъектов вводится режим ограничения доступа. Доступ к персональным данным имеют только те работники, которым они необходимы в связи с исполнением ими трудовых обязанностей и только в необходимом объеме.

Безопасность персональных данных при их обработке в ИСПДн-ах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры, средства защиты информации, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, а также используемые информационные технологии защиты.

Для защиты конфиденциальной информации создаются неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося осуществить несанкционированный доступ и овладеть информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только получение ценных сведений и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Технические и программные средства используемые, для защиты информации, должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим необходимый уровень защиты.

Обязательным условием защиты информации является осуществление внутреннего контроля соответствия обработки персональных данных.

Заключительная часть

Безразличие работников к вопросам безопасности, не понимание ими важности соблюдения установленных правил, ценности той информации, к которой имеют доступ, и является основной причиной утечек персональных данных.

В случае обнаружения нарушений, связанных с обработкой и защитой персональных данных необходимо немедленно проинформировать о данном факте лиц ответственных за их защиту.

За дополнительными разъяснениями вопросов касающихся применения законодательства в области обработки персональных данных следует обращаться в отдел по защите информации.

Отдел по защите информации УКДиПО.