Меры по защите персональных данных работников и обучающихся

Любое юридическое лицо в силу требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обязано принимать меры по защите персональных данных, при этом перечень таких мер оно вправе определять самостоятельно.

Мероприятия по защите персональных данных можно разделить на две большие подгруппы:

- по внутренней;
- внешней защите персональных данных.

К мерам по внутренней защите персональных данных относятся следующие действия:

- ограничение числа работников (с регламентацией их должностей), которым открыт доступ к персональным данным;
- назначение ответственных лиц за обработку ПД, обеспечивающих этот процесс и лиц контролирующих отсутствие нарушений действующего законодательства;
- утверждение перечня документов, содержащих персональные данные;
- издание внутренних документов по защите персональных данных, осуществление контроля за их соблюдением;
- ознакомление работников с действующими нормативами в области защиты персональных данных и локальными актами;
- проведение проверок соответствующих знаний работников, обрабатывающих персональные данные, и соблюдения ими требований действующего законодательства и нормативных документов по защите конфиденциальных сведений;
- рациональное размещение рабочих мест для исключения несанкционированного использования защищаемой информации;
- утверждение списка лиц, имеющих право доступа в помещения, в которых хранятся персональные данные;
- утверждение порядка уничтожения информации;
- выявление и устранение нарушений требований по защите персональных данных;
- проведение профилактической работы с сотрудниками по предупреждению разглашения ими персональных данных.

Среди мер по внешней защите персональных данных следует выделить такие:

- введение пропускного режима, порядка приема и учета посетителей;
- внедрение технических средств охраны, программных средств защиты информации на электронных носителях.

Иные организационные и технические меры, направленные на защиту персональных данных

Необходимы организационные и технические меры, предназначенные для защиты персональных данных. Вот как выглядит их список:

- требования к помещению, где хранятся персональные данные. Следует иметь в виду, что законодательством они не установлены. Однако если исходить из имеющихся аналогичных законов, учитывать положения Трудового кодекса РФ, то во избежание несанкционированного доступа к персональным данным на бумажных носителях необходимо оборудовать помещение, где они хранятся, запирающимися шкафами. В локальном нормативном акте устанавливаются помещения, где обрабатываются персональные данные, и утверждается перечень лиц, имеющих допуск к ним;
- При обеспечении программной защиты информационной системы образовательной организации (в случае использования электронных систем обработки персональных

данных) учитываются требования по обеспечению безопасности таких данных, отраженные в Положении об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных образовательного учреждения. Ограничен доступ к определенным сведениям в информационных системах (например, - пароли и т. д.), электронным базам данных, содержащим персональные данные работников и обучающихся, двухуровневой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли должны устанавливаться администратором баз данных и администратором, соответственно, сообщаться индивидуально сотрудникам, имеющим доступ к персональным данным, при этом меняются они достаточно часто (ежегодно);

– В целях соблюдения конфиденциального режима работы с персональными данными ведется журнал учета выдачи персональных данных другим лицам, организациям и государственным органам. В нем регистрируются поступающие запросы, а также сведения о лице, направившем запрос, дате передачи персональных данных или факт уведомления об отказе в их предоставлении, а также отмечается, какая именно информация была передана.

Передача персональных данных третьим лицам

Поводов для передачи персональных данных третьим лицам может быть много – заключение договоров дополнительного медицинского страхования, получение «зарплатных» банковских карт и т. д. Согласие на обработку персональных данных получается с каждого работника.

Какие контрольные органы вправе затребовать персональные данные

Суды и другие правоохранительные органы могут беспрепятственно получать от образовательного учреждения персональные данные сотрудников, клиентов или контрагентов без согласия последних.

Однако не все органы могут беспрепятственно получать доступ к ПДн.

ПРИМЕР: Девятый арбитражный апелляционный суд в своем постановлении от 25.06.09 г. по делу № А40-76345/08-122-112 указал, что сотрудник службы судебных приставов не имеет права запрашивать и получать сведения, содержащие личные данные граждан. В частности, суд отметил, что ни Федеральный закон от 21.07.1997 № 118-ФЗ «О судебных приставах», ни Федеральный закон от 02.01.2007 № 229-ФЗ «Об исполнительном производстве» не предоставляют судебным приставам-исполнителям права получать персональные данные без согласия их субъектов, не устанавливают условия получения таких данных, не определяют круг субъектов, персональные данные которых подлежат обработке, а также полномочия судебного пристава исполнителя по их обработке.

Трансграничные передачи

Что такое трансграничная передача данных? Это передача персональных данных оператором через государственную границу Российской Федерации органу власти, физическому или юридическому лицу иностранного государства. В Российской Федерации одним из критериев оценки государства с точки зрения организации им адекватного уровня защиты может выступать факт ратификации им Конвенции о защите прав физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г., ETS № 108.

До начала передачи оператор должен убедиться в том, что на территории иностранного государства обеспечена адекватная защита прав субъектов персональных данных.

Камнем преткновения является формулировка «адекватная защита», так как критерии адекватности нигде не определяются, при этом здравый смысл подсказывает, что адекватной можно считать защиту, которая соответствует российскому законодательству.

Присоединение иностранного государства к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 1981 г.; с изменениями 1999 г.) позволяет причислять его к числу тех, кто гарантирует вполне адекватную защиту. Но, например, США эту конвенцию не ратифицировали. Есть такая программа U.S. – EU Safe Harbor. Она упорядочивает отношения только между ЕС и США. Мы же в ЕС не входим. В США законодательства, регулирующего область персональных данных, как такового не существует. Есть только упоминание в законах штатах о так называемом privacy (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:).

Хранение ПДн

Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении 75-летнего срока их хранения, если иное не определено законом.

Согласно ФЗ-152, персональные данные должны быть уничтожены оператором по достижении цели их обработки. А, например, первичные документы по кадровому учету и заработной плате необходимо хранить в течение 75 лет. Но они должны находиться в архиве, а ФЗ-152 на архив не распространяется в соответствии с законом об архиве. Таким образом, после сдачи документов в архив организация уже не может хранить эти сведения у себя.

Что касается больничных листов, то это касается субъекта. К примеру, если работник уволился, заново никуда устроиться не успел и заболел, то больничный рассчитывается ему на основании дохода по последнему месту работы. А в организации в соответствии с налоговым законодательством обязаны хранить все финансовые документы за пять прошедших лет для налоговой проверки. Причем отсчет срока хранения ведется от начала нового финансового года или даты передачи дела в архив, а это тоже обычно происходит в конце года. И кстати, до пяти лет допускается хранение документов в организации, без передачи их в архив (*Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»*)

В новом постановлении № 1119 объединены два проекта, один из которых определяет уровни защищенности информации, содержащей персональные данные, а второй – требования к их безопасности. Постановление определяет, что набор средств защиты ПДн оператор должен выбирать самостоятельно, основываясь на ранее принятых нормативных актах ФСБ и ФСТЭК.

Согласно документу, актуальными угрозами для безопасности персональных данных являются условия и факторы, создающие потенциальную опасность несанкционированного доступа к базам данных при их обработке, в результате которого данные могут быть уничтожены, изменены, заблокированы или предоставлены третьим лицам, не имеющим к ним права доступа. Кроме того, в постановлении определены три типа угроз информационным системам, содержащим пользовательские базы данных, а также четыре уровня защищенности информационных систем.

Подробной классификации угроз нет, поэтому проводится их самостоятельная оценка и устанавливается соответствующий уровень защищенности в целях их нейтрализации. Для обеспечения нужного уровня защищенности необходимо реализовать ряд организационных и технических мероприятий по выбору средств защиты информации, делается это, ориентируясь на документы ФСБ и ФСТЭК.