Закон национального уровня, принятый 23.12.2010 под индексом № 359-ФЗ, регламентирует, что все ИСПд должны быть сведены к единому образцу с июля 2011 года. Современные образовательные учреждения занимаются воплощением в жизнь этого требования, с учетом поправок и изменений, периодически вносимых законодательными органами.

**Правовая основа работы с персональными данными**

Школы, университеты, среднеспециальные учебные заведения логично стали основной базой для внедрения новейших систем обработки персональных данных. Образовательные учреждения предназначены для подготовки кадров, адаптированных к электронному делопроизводству и в качестве преподавателей, и в роли рядовых пользователей. Общая культура безопасности данных должна прививаться гражданам в любом возрасте без исключения, а общеобразовательные учреждения – первое место, где может культивироваться уважение к закону в общем, и к конфиденциальности приватной информации в частности. Именно в сфере образования лучше всего внедряется понимание законности или незаконности оперирования данными о гражданине.

Защита персональных данных включает как юридический, так и технический аспекты правового регламентирования. Электронное обеспечение сбора информации – технический вопрос, а сама организация процесса относится в большей степени к вопросам делопроизводства, чем к актуальной юридической практике.

Защита ПДн работников (учителей, научных сотрудников, административных штатных единиц, системных администраторов и иного техперсонала) подпадает под действие следующих законодательных актов:

Конституции РФ;

Закона № 149-ФЗ, описывающего защиту данных в аспекте информтехнологий и сами информационные технологии;

Закона № 152-ФЗ, регламентирующего правовое положение персональных данных;

ТК РФ;

многочисленных ведомственных и подзаконных правовых актов.

Третья статья закона № 152-ФЗ подразумевает под «персональными данными» любые биографические данные по субъекту – физическому лицу:

его полное имя;

год и число рождения;

фактический адрес и место регистрации;

профессию и квалификационные навыки гражданина;

уровень и время получения образования;

размеры доходов и объем уплаченного налога;

социальное положение;

недвижимые и иные активы;

семейный статус и прочие социальные, финансовые, юридические факты о гражданине.

Вторая статья этого же закона допускает обработку персональных данных исключительно в объемах, необходимых для обеспечения рабочего процесса, с гарантией неприкосновенности приватной жизни. Этот же закон регламентирует все требования по обращению с конфиденциальной информацией. Распространяется ФЗ № 152 на все организации на территории РФ, включая учебные учреждения, которые являются операторами по обработке персональных данных. 19-я статья этого документа определяет, что именно на оператора возлагаются все организационные и технические вопросы как по сбору, так и по защите потенциально уязвимого приватного материала.

17.11.2007 № 781 исполнительная власть одобрила Положение, касающееся безопасности ПД в условиях применения электронных систем. В этом нормативном акте описан полный комплекс необходимой материальной части, к которой непосредственно относятся:

записывающая аппаратура;

принимающие персональную информацию терминалы;

элементы используемых сетей и все сопутствующее этой работе ПО.

Конкретные версии программ и модели оборудования оговариваются особо в профильных документах, составленных Минобразования и специальными уполномоченными органами.

Статья 22 Закона № 152-ФЗ требует от оператора обязательного уведомления компетентных органов непосредственно перед началом обработки персональных данных. Процедура необходима для предотвращения потенциальных злоупотреблений, нарушений и контроля над выполнением образовательными учреждениями требований законодательства в сфере обработки ПДн.

В качестве уполномоченного органа законодательство РФ определяет Россвязькомнадзор, который в 2008 году разработал и заверил соответствующие образцы Уведомления о начале обработки ПДн и Рекомендации по их оформлению. Оператор может не уведомлять Россвязькомнадзор, если граждане, предоставляющие свои персональные данные оператору, находятся с ним в трудовых отношениях. Университет, колледж, иное образовательное учреждение могут осуществлять такую деятельность относительно преподавателей без создания Уведомления.

**Действия по защите персональных данных**

Образовательные учреждения при разработке мероприятий по защите ПДн привлекают к обработке персональных данных юристов, кадровиков, создают отделы компьютерных технологий.

Юридическую часть и направления работы в этой сфере составляют операции по:

разработке локальных актов, которые будут регламентировать организацию, юридическую, техническую часть деятельности с ПДн;

определению процедуры взаимодействия со всеми надзорными органами;

распределению функций между сотрудниками, закреплению между ними задач по ведению документооборота, обработке, хранению персональных данных.

Специфика учебных заведений требует обрабатывать личные данные не только учащихся, но и их родителей, если речь идет о первичных уровнях российских учебных заведений.

Процедура передачи конфиденциальных данных третьим лицам нуждается в особом подходе:

основаниями для подобных действий могут быть требования федерального законодательства, органов правосудия;

получение письменного согласия субъекта ПДн;

заключение договора с третьими лицами, в котором должны содержаться их заверения в обеспечении полной конфиденциальности и сохранности данных в процессе обработки.

Такие же требования должны соблюдаться при работе с ПДн при обработке с помощью компьютерной техники, интернет-ресурсов общеобразовательных учреждений.

**Обязанности работодателей в вопросах защиты ПДн**

Работодатель, в соответствии со статьей 21 ФЗ № 152, должен:

заблокировать ПДн работника образовательного учреждения по его требованию или требованию его законных представителей, если такая информация не является достоверной, с ней проводились незаконные действия, оператор должен уточнить или изменить такие данные на основании предоставленной субъектом информации;

исправить нарушения, если они были найдены в течение не более 3 рабочих дней, начиная со дня их выявления. Если устранить их в течение этого периода времени нет возможности, оператор должен уничтожить эти сведения. Информацию об устранении нарушений, выполнении процедуры уничтожения ПДн работодатель должен направить субъекту, его представителям или уполномоченному органу;

незамедлительно остановить обработку ПДн, уничтожить их, если субъект отозвал свое согласие на эти действия на протяжении 3 рабочих дней после получения уведомления, если другое не предусматривается законодательством.

**Этапы защиты персональных данных**

Анализ необходимости и объемов обработки ПДн.

Анализ и определение информационных процессов обработки конфиденциальной информации.

Создание перечня отделов и штатных единиц, задействованных в обработке персональных сведений.

Суммирование информсистем и анализируемых вводных.

Определение категорий собираемой в будущем информации.

Издание пакета распорядительных документов по обработке ПДн.

Разработка эффективной системы безопасности.

**Локальная защита ПДн работников общеобразовательных учреждений**

Ст. 85 ТК РФ трактует конфиденциальной информацией данные о штатных единицах и все запрашиваемые сведения по штатным сотрудникам образовательного учреждения, необходимые оператору для совершения действий, прописанных в трудовых договорах. Какие конкретно сведения подлежат защите и относятся к категории конфиденциальных, должен решать сам работодатель, учитывая текущее законодательство. Статья 87 ТК РФ требует разработки, внедрения и поддержания работодателем процедуры архивирования, сохранности и обработки ПД сотрудников.

Первичным документом выступает Положение о сборе и защите ПДн сотрудников, в ходе имплементации которого обязательно учитывается мнение уполномоченных профсоюзных ячеек в соответствии с требованиями статьи 372 ТК РФ. В этом законодательном акте регламентирован порядок оперирования персональными данными, содержатся методики и принципы обеспечения базовых информационных прав штатных сотрудников, определение ответственных лиц и рангов доступности ПДн по разным категориям штатных сотрудников, определение санкций за нарушения, допущенные в работе с ПДн сотрудников.

Составление Положения – обязанность, которую необходимо выполнить оператору ПДн, отсутствие этого документа квалифицируется как прямое нарушение оператором федеральных законов.

Защита персональных данных в образовательном учреждении состоит из следующих мероприятий:

при получении конфиденциальной информации необходимо письменное согласие от собственника ПДн на их обработку, а также на возможность передачи этих данных третьим лицам в рамках действующего законодательства и в объемах, необходимых для выполнения его требований и реализации рабочего процесса в образовательном учреждении;

во время хранения ПДн требуется издать приказ об ответственных лицах из числа персонала, которые будут иметь доступ к этим документам, включая приватные данные, не подлежащие разглашению.

Работодатель (руководитель образовательного учреждения) – юридический объект, который отвечает за конфиденциальность данных, полученных для обработки в рамках трудовых взаимоотношений. В его ведении должны находиться соответствующие журналы контрольного внутреннего и исходящего учета персональных данных, содержащие, помимо описи конфиденциальных документов, порядок их изъятия из хранилища и передачи в третьи руки. В число этих лиц входят как представители различных юрлиц, так и государственные контрольно-надзорные органы, инстанции правопорядка, представители судебной системы.

Непосредственно сам Журнал учета внутреннего доступа к персональным данным (наименование условно и регламентации отдельно не подлежит, главное, чтобы оно точно указывалось в отчетной документации) должен содержать:

даты документооборота личных дел (выдача-возврат);

срок пользования;

цели, с которыми документ выдавался;

сам перечень выдаваемых документов.

Сотрудник, который работает с личным делом другого сотрудника, ни в коем случае не имеет права вносить в документ какие-либо правки.

Образовательное учреждение должно вести Журнал учета наружного оборота персональных данных работников, содержащий все поступающие запросы, информацию о том, кто этот запрос направил в учреждение, дату начала документооборота по делу либо пометку об отказе выдать интересующие сведения, также указывать конкретную переданную информацию.

Качественная система учета персональных данных требует проведения периодических проверок наличия личных дел и иных носителей конфиденциальной персональной информации, установления четкого порядка документооборота.