Особенности защиты персональных данных в образовательных учреждениях

Согласно Федеральному закону от 23.12.2010 № 359-ФЗ информационные системы персональных данных, созданные до 1 января текущего года, должны быть приведены в соответствие с установленными требованиями не позднее 1 июля 2011 г.

Законодательное обеспечение защиты персональных данных

В настоящее время в образовательных учреждениях (далее – ОУ) активно внедряются информационные системы, осуществляющие обработку персональных данных, делопроизводство, бухгалтерские программы и др. Эти системы предназначены для ведения базы данных воспитанников, обучающихся, родителей и работников ОУ, оперативного управления учреждением. Образовательные учреждения должны отреагировать на требования законодательства о защите персональных данных участников образовательного процесса в первую очередь, т. к. речь идет о защите сведений, незаконное использование которых может серьезно отразиться на правах граждан.

Защита персональных данных работника является неотъемлемой составляющей права на уважение частной жизни человека, которое может быть ограничено только в предусмотренных пределах и при определенных условиях.

Защита персональных данных представляет собой комплекс мер технического, организационного, организационно-технического и правового характера, направленных на защиту сведений, относящихся к определенному или определяемому на основании такой информации физическому лицу – субъекту персональных данных (работнику).

Положения о защите персональных данных работников регламентируются:

Конституцией Российской Федерации;

Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ);

Трудовым кодексом РФ (далее – ТК РФ).

Кроме того, в целях обеспечения защиты персональных данных работников в соответствии с этими федеральными законами приняты подзаконные нормативные правовые акты (постановления Правительства РФ, ведомственные нормативные правовые акты).

В соответствии со ст.3 Закона № 152-ФЗ персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных): фамилия, имя, отчество; год, месяц, дата и место рождения; адрес;

семейное, социальное, имущественное положение; образование, профессия, доходы и другая информация.

Согласно ст.2 Закона № 152-ФЗ его целью является защита прав и свобод человека и гражданина при обработке его персональных данных, в т. ч. защита прав на неприкосновенность частной жизни, личную и семейную тайну.

Персональные данные относятся к категории конфиденциальной информации, которые указаны в Перечне сведений конфиденциального характера, утвержденном указом Президента РФ от 06.03.1997 № 188. Следовательно, работодатель, получающий доступ к персональным данным, должен обеспечить их конфиденциальность.

Закон № 152-ФЗ определяет требования к сбору и обработке (хранению, актуализации, использованию, раскрытию и предоставлению) персональных данных физических лиц во всех сферах, где используются персональные данные, в т. ч. в сфере трудовых правоотношений.

Требования закона распространяются на все организации (независимо от формы собственности), в т. ч. на ОУ, которые выступают операторами, обрабатывающими в своих информационных системах персональные данные физических лиц (работников, обучающихся и др.).

Вопрос правовой регламентации обеспечения защиты персональных данных работников в настоящее время особенно актуален, поскольку информационные системы персональных данных работников ОУ, созданные до 1 января 2010 г., должны быть приведены в соответствие с требованиями Закона № 152-ФЗ не позднее 1 января 2011 г. – они должны представлять собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием или без использования средств автоматизации.

В соответствии с ч.1 ст.19 Закона № 152-ФЗ оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Постановлением Правительства РФ от 17.11.2007 № 781 утверждено Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, в т. ч. с использованием средств автоматизации. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами

данных и т. п.), средства защиты информации, применяемые в информационных системах.

В соответствии с ч.3 ст.4 Закона № 152-ФЗ постановлением Правительства РФ от 15.09.2008 № 687 утверждено Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации. Данное Положение предусматривает, что обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований этого Положения.

Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 05.02.2010 № 58 утверждено Положение о методах и способах защиты информации в информационных системах персональных данных, которое подробно регламентирует вопросы, связанные с порядком применения методов и способов защиты информации в информационных системах персональных данных оператором или уполномоченным им лицом.

В соответствии с ч.1 ст.22 Закона № 152-ФЗ оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, за исключением случаев, предусмотренных ч. 2 указанной статьи.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Россвязькомнадзор) выступает таким уполномоченным органом, который приказом от 19.08.2011 № 706 утвердил образец Уведомления об обработке (о намерении осуществлять обработку) персональных данных и Рекомендации по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных.

Частью 2 ст.22 Закона № 152-ФЗ установлено, что оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных, относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения. Следовательно, образовательные учреждения не должны уведомлять этот уполномоченный орган об обработке ими персональных данных работников, состоящих в трудовых отношениях с учреждениями.

Планирование мероприятий по защите персональных данных

При планировании в ОУ мероприятий, связанных с защитой персональных данных, рекомендуется привлекать юристов, специалистов отдела кадров и по информационной работе (компьютерным технологиям).

Правовая составляющая должна стать обязательным элементом всей деятельности учреждения в этом направлении, поскольку необходимо:

разработать локальные акты (нормативные и правовые), связанные не только с организационной и правовой, но и с технической защитой персональных данных;

сформировать механизмы взаимоотношений с органами, осуществляющими управление в сфере образования, профсоюзными организациями, органами контроля и надзора и т. д.

Главным условием защиты персональных данных является четкая регламентация функций работников, а также принадлежности работникам документов, дел, картотек, журналов персонального учета и баз данных.

Далее ключевым вопросом становится оценка наличия предусмотренных законодательством оснований для обработки персональных данных, а в случаях, когда они отсутствуют, – получение согласия субъекта персональных данных на их обработку. При этом согласно Закону № 152-ФЗ обязанность доказательства согласия субъекта персональных данных на их обработку возлагается на оператора, т. е. на работодателя.

Несмотря на то, что в данном комментарии речь идет исключительно о защите персональных данных работников, хотелось бы в контексте обратить внимание на то, что в ОУ обрабатываются персональные данные обучающихся и их родителей, поэтому ОУ предварительно должно получить согласие родителей на обработку персональных данных их самих и их детей.

Следует уделить особое внимание процедуре передачи персональных данных третьим лицам. Для этого необходимо наличие:

основания для такой передачи, предусмотренного федеральными законами, или согласия субъекта персональных данных, закрепленного, например, в договоре на оказание услуг;

договора с этим третьим лицом, существенным условием которого должна быть обязанность обеспечения указанным лицом конфиденциальности и безопасности персональных данных при их обработке.

Необходимо очень внимательно подойти к вопросу размещения информации, содержащей персональные данные, на интернет-сайте ОУ.

С учетом выше изложенного можно выделить следующие обязательные этапы работы по защите персональных данных работников:

1) определение всех ситуаций, когда требуется проводить обработку персональных данных;

2) выделение процессов, в которых обрабатываются персональные данные;

3) выбор ограниченного числа процессов для проведения аналитики (на этом этапе формируется перечень подразделений и работников, участвующих в обработке персональных данных в рамках своей служебной деятельности);

4) определение круга информационных систем и совокупности обрабатываемых персональных данных;

5) проведение категорирования персональных данных и предварительной классификации информационных систем;

6) разработка пакета организационно-распорядительных документов для обеспечения защиты персональных данных (положения, приказы, акты, инструкции и т. п.);

7) внедрение системы обеспечения безопасности информации.

Следовательно, защита персональных данных работников в образовательном учреждении, по сути, сводится к созданию режима обработки персональных данных, включающего:

создание внутренней документации по работе с персональными данными;

организацию системы защиты персональных данных;

внедрение технических мер защиты персональных данных.

Правовое регулирование вопросов обеспечения защиты персональных данных работников на локальном уровне

В соответствии со ст.85 ТК РФ к персональным данным работника относится информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Вопрос о том, какая необходимая работодателю информация из категории персональных данных работника подлежит защите, работодатель должен решить самостоятельно с учетом действующего законодательства и с участием самих работников и их представителей.

Статьей 87 ТК РФ предусмотрено, что порядок хранения и использования персональных данных работников устанавливается работодателем с учетом требований ТК РФ и иных федеральных законов, что подразумевает регулирование порядка обработки персональных данных работников локальными нормативными и иными актами.

Основным таким локальным нормативным актом должно быть Положение о защите персональных данных работников, которое принимается с учетом мнения выборного органа первичной профсоюзной организации учреждения в порядке, предусмотренном ст.372 ТК РФ.

Этот документ определяет: порядок обработки персональных данных работников; обеспечение защиты прав и свобод работников при обработке их персональных данных; ответственность лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

Данный локальный нормативный акт является обязательным, поэтому его отсутствие может быть квалифицировано государственным органом контроля и надзора как нарушение работодателем трудового законодательства.

Наряду с Положением о защите персональных данных работников в образовательном учреждении также необходимо наличие следующих документов:

в процессе получения персональных данных – согласие работника на получение работодателем персональных данных от третьих лиц и уведомление работника о получении его персональных данных от третьих лиц;

при обработке персональных данных – согласие работника на обработку его персональных данных; персональных данных работников;

при хранении персональных данных – приказ об утверждении списка лиц, имеющих доступ к персональным данным работников, и обязательств о неразглашении;

при передаче персональных данных работников – согласие работника на передачу его персональных данных третьим лицам.

Поскольку на работодателя возложена обязанность соблюдения режима конфиденциальности персональных данных, в целях обеспечения его выполнения необходимо вести журналы учета персональных данных, их выдачи и передачи другим лицам и представителям различных организаций, органам контроля и надзора, правоохранительным органам, которые обеспечат документальную фиксацию внутреннего и внешнего доступа к персональным данным работников.

В Журнале учета внутреннего доступа к персональным данным (доступа работников учреждения к персональным данным других работников) следует указывать такие сведения, как: даты выдачи и возврата документов (личных дел); срок пользования; цели выдачи; наименование выдаваемых документов. Лицо, которое возвращает документ, содержащий персональные данные, должно обязательно присутствовать при проверке наличия всех имеющихся документов по описи, если выданные документы составлены более чем на одном листе.

Лицо, которое получает личное дело другого работника во временное пользование, не имеет права делать в нем какие-либо пометки, исправления, вносить новые записи, извлекать документы из личного дела или помещать в него новые.

Помимо этого также необходимо вести Журнал учета выдачи персональных данных работников организациям и государственным органам, в котором необходимо регистрировать: поступающие запросы, сведения о лице, направившем запрос; дату передачи персональных данных или уведомления об отказе в их предоставлении; какая именно информация была передана.

Система учета персональных данных может предусматривать проведение регулярных проверок наличия документов и других носителей информации, содержащих персональные данные работников, а также устанавливать порядок работы с ними. В этой связи необходимо ведение

журнала проверок наличия документов, содержащих персональные данные работников.

Таким образом, рекомендуется ведение в ОУ следующих учетных документов движения персональных данных работников:

Журнал учета внутреннего доступа к персональным данным работников в учреждении;

Журнал учета выдачи персональных данных работников учреждения организациям и государственным органам (Журнал учета внешнего доступа к персональным данным работников);

Журнал проверок наличия документов, содержащих персональные данные работников.

Кроме того, поскольку к методам и способам защиты информации от несанкционированного доступа для обеспечения безопасности персональных данных в информационных системах определенного класса относится учет всех защищаемых носителей информации (с помощью их маркировки и занесения учетных данных в журналы учета), необходимо также ведение ***Журнала учета применяемых работодателем носителей информации.***

Обязанности работодателя по обеспечению защиты персональных данных работников

В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника в соответствии со ст. 86 ТК РФ обязаны соблюдать необходимые требования. В соответствии со ст. 21 Закона № 152-ФЗ оператор (работодатель) также обязан:

1) осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента обращения субъекта персональных данных или его законного представителя либо получения запроса уполномоченного органа по защите прав субъектов персональных данных в случае выявления недостоверных персональных данных или неправомерных действий с ними оператора на период проверки.

В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование;

2) устранить допущенные нарушения в случае выявления неправомерных действий с персональными данными в срок, не превышающий трех рабочих дней с даты такого выявления. В случае невозможности устранения допущенных нарушений в указанный срок оператор обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае если

обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных – также указанный орган;

3) незамедлительно прекратить обработку персональных данных и уничтожить их в срок, не превышающий трех рабочих дней с даты достижения цели обработки, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта персональных данных или его законного представителя, а в случае поступления обращения или запроса от уполномоченного органа по защите прав субъектов персональных данных – также указанный орган;

4) прекратить обработку персональных данных и уничтожить их, в случае отзыва субъектом персональных данных согласия на их обработку, в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

Порядок передачи работодателем персональных данных работников

Персональные данные работника не могут быть переданы работодателем третьей стороне. Исключением из данного правила являются следующие случаи:

выдача работником письменного согласия на передачу персональных данных третьей стороне;

передача персональных данных работника в целях предупреждения угрозы жизни и здоровью самого работника;

другие случаи, установленные федеральным законом.

При передаче персональных данных работника работодатель должен соблюдать следующие обязательные требования, предусмотренные ст. 88 ТК РФ:

не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных ТК РФ или иными федеральными законами;

разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;

передавать персональные данные работника представителям работников в порядке, установленном ТК РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

Поскольку персональные данные относятся к категории конфиденциальной информации, лица, получившие персональные данные работника на законном основании, обязаны использовать их исключительно в целях, которые заявлялись при запросе соответствующей информации, а также не разглашать такую информацию (исключения из данного правила определяются только федеральными законами).

Получателями персональных данных работника на законном основании являются:

1)органы социального страхования, органы пенсионного обеспечения, а также иные органы, организации и граждане (в соответствии с Федеральным законом от 16.07.1999 № 165-ФЗ «Об основах обязательного социального страхования», согласно которому отношения по обязательному социальному страхованию возникают у страхователя (работодателя) – по всем видам обязательного социального страхования с момента заключения с работником трудового договора);

2)налоговые органы (в соответствии со ст.24 Налогового кодекса РФ, выступая в качестве налогового агента работников, исчисляющего, удерживающего из средств, выплачиваемых работникам, и перечисляющего в бюджет соответствующие налоги, работодатель обязан представлять в налоговый орган по месту своего учета документы, необходимые для контроля за правильностью исчисления, удержания и перечисления налогов);

3)органы прокуратуры и другие правоохранительные органы (в соответствии со ст.23 Закона № 152-ФЗ они имеют право запрашивать информацию у работодателей в рамках проверки для решения вопроса о возбуждении: дела об административном правонарушении; уголовного дела по признакам правонарушений (преступлений), связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью);

4)федеральная инспекция труда (в соответствии со ст.357 ТК РФ государственные инспекторы труда при осуществлении надзорно-контрольной деятельности имеют право запрашивать у работодателей и безвозмездно получать от них документы и информацию, необходимую для выполнения надзорных и контрольных функций, включая персональные данные работников);

5) профессиональные союзы (в соответствии с Федеральным законом от 12.01.1996 № 10-ФЗ «О профессиональных союзах, их правах и гарантиях деятельности» и ТК РФ профсоюзы имеют право на получение информации от работодателей по социально-трудовым вопросам для осуществления своей уставной деятельности, а также на осуществление общественного контроля за соблюдением работодателями, должностными лицами трудового законодательства);

6) другие органы и организации в случаях, предусмотренных федеральным законом.

Права и обязанности работников, связанные с обработкой и защитой их персональных данных

В соответствии с п.8 ст.86 ТК РФ работники и их представители должны быть ознакомлены под роспись с документами, устанавливающими порядок обработки и защиты персональных данных, а также их права и обязанности в этой области. Работники в соответствии со ст.89 ТК РФ имеют право:

– на полную информацию о своих персональных данных и обработке этих данных;

– свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

– определение своих представителей для защиты персональных данных;

– доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

– требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

– обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

Работники обязаны в разумный срок информировать работодателя об изменении персональных данных.

Ответственность за нарушение требований по защите персональных данных

В соответствии со ст.24 лица, виновные в нарушении требований этого федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность Закона № 152-ФЗ.

Неисполнение требований Закона № 152-ФЗ операторами баз данных может повлечь:

гражданские иски со стороны работников;

репутационные риски;

приостановление или прекращение обработки персональных данных, осуществляемой с нарушением требований Закона № 152-ФЗ;

направление в органы прокуратуры, другие правоохранительные органы материалов для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных; привлечение к административной и уголовной ответственности лиц, виновных в нарушении соответствующих статей Уголовного кодекса РФ и Кодекса РФ об административных правонарушениях.

В соответствии со ст.90 ТК РФ, устанавливающей ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника, виновные в этом лица привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном ТК РФ и иными федеральными законами.

Так, к работнику, отвечающему за хранение персональных данных в силу его трудовых обязанностей, работодатель вправе применить одно из дисциплинарных взысканий, предусмотренных ст.192 ТК РФ (замечание, выговор, увольнение).

Работодатель может расторгнуть трудовой договор по своей инициативе по подп. «в» п.6 ч.1 ст.81 ТК РФ при разглашении работником охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в т. ч. в случае разглашения персональных данных другого работника.

Помимо этого работники, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, могут быть привлечены к материальной и уголовной ответственности.

Система государственного надзора и контроля в области персональных данных

Система государственного надзора и контроля в области персональных данных строится на функционировании трех регуляторов, ответственных за определенные области деятельности в сфере персональных данных.

Основным регулятором, осуществляющим контроль и надзор за соответствием обработки персональных данных требованиям законодательства РФ в этой области, является уполномоченный орган по защите прав субъектов персональных данных – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), территориальные органы которой действуют в каждом субъекте РФ. Зона ответственности и область проверок этого регулятора – все организационные мероприятия, включая акт классификации информационных систем персональных данных. Права и обязанности этого уполномоченного органа устанавливаются положением о нем в соответствии со ст.23 Закона № 152-ФЗ.

Вторым регулятором, контролирующим осуществление мер по технической защите информационных систем обработки персональных данных, является Федеральная служба по техническому и экспортному контролю (ФСТЭК) и ее территориальные органы. Сфера ответственности и область проверок – технические средства защиты информации, использующие некриптографические методы и способы защиты персональных данных.

Третьим регулятором является федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, – Федеральная служба безопасности РФ (ФСБ России), которая устанавливает особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах и осуществляет контроль в этой области.

Кроме того, следует иметь в виду, что в соответствии со ст.354 ТК РФ Федеральная инспекция труда, состоящая из федерального органа исполнительной власти и его территориальных органов (государственных инспекций труда), является уполномоченным органом на проведение государственного надзора и контроля за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, в т. ч. и по вопросам защиты персональных данных работников.