Утверждено
приказом ФБУ Волгоградская ЛСЭ
Минюста России
от 24 июня 2016 г. № 20

Положение об обработке и защите персональных данных в федеральном бюджетном учреждении Волгоградская лаборатория судебной экспертизы Министерства юстиции Российской Федерации

1. Общие положения

1.1 Настоящее Положение определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в федеральном бюджетном учреждении Волгоградская лаборатория судебной экспертизы Министерства юстиции Российской Федерации (далее по тексту - Учреждение) персональных данных, функции Учреждения при обработке персональных данных, права субъектов персональных данных, а также реализуемые в Учреждении требования к защите персональных данных и ответственность должностных лиц Учреждения, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, правила обработки персональных данных (ПДн), порядок уничтожения ПДн, правила осуществления внутреннего контроля соответствия обработки ПДн требованиям законодательства, правила доступа субъектов ПДн к своим персональным данным, находящимся в информационных системах персональных данных (ИСПДн) и другие вопросы, возникающие при обработке ПДн в Учреждении.

Действие настоящего Положения не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования, содержащие персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.

1.2. Целью данного Положения является обеспечение выполнения требований законодательства Российской Федерации в области защиты персональных данных и защита прав и свобод субъектов ПДн при обработке их персональных данных в Учреждении.

1.3. Основные понятия, используемые в настоящем Положении.

В настоящем Положении используются следующие основные термины и определения.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Информация - сведения (сообщения, данные) независимо от формы их представления.

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и

(или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемые 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.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

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

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку с помощью информационных технологий и технических средств.

2. Принципы, условия и цели обработки персональных данных

2.1. Принципы обработки персональных данных в Учреждении.

Обработка персональных данных в Учреждении осуществляется с учетом необходимости обеспечения защиты прав и свобод субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

а) обработка персональных данных осуществляется в Учреждении на законной и справедливой основе;

б) обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;

в) не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

г) не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

е) обработке подлежат только персональные данные, которые отвечают целям их обработки;

ж) содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;

з) при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Учреждением принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

и) хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Условия обработки персональных данных в Учреждении.

Обработка персональных данных в Учреждении осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

2.2.1. Учреждение без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральными законами.

2.2.2. Учреждение вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.2.3. В целях внутреннего информационного обеспечения Учреждение может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, адрес электронной почты, адрес

проживания и регистрации, иные персональные данные, указанные в его письменном согласии.

2.2.4. Учреждением обрабатываются персональные данные, принадлежащие работникам Учреждения.

2.2.5. Общедоступные персональные данные, обрабатываемые в Учреждении, содержат сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом.

2.2.6. Специальные категории персональных данных, к которым относится информация о национальной и расовой принадлежности субъекта, о религиозных, философских, либо политических убеждениях, информация о здоровье и интимной жизни субъекта и биометрические персональные данные в Учреждении не обрабатываются. Перечень персональных данных работников Учреждения, обрабатываемых в Учреждении в связи с реализацией трудовых отношений, приведены в Приложении №1 к настоящему Положению.

2.3. Цели обработки персональных данных в Учреждении.

2.3.1. Персональные данные обрабатываются в Учреждении в целях:

а) выполнения требований действующего Законодательства Российской Федерации, в части передачи, обработки и предоставления полученных персональных данных, в связи с приемом граждан на работу в Учреждение;

б) организации кадрового учета Учреждения, в том числе воинского учета, исполнения обязательств по трудовым и гражданско-правовым договорам с работниками;

в) обеспечения деятельности бухгалтерии Учреждения по начислению и регулярной выплате заработной платы работникам;

г) заключения, исполнения и прекращения гражданско-правовых договоров с физическими и юридическим лицами, в случаях, предусмотренных действующим законодательством и Уставом Учреждения;

д) выполнения требований по предоставлению обрабатываемых персональных данных субъектов в Министерство юстиции Российской Федерации, в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, в иные государственные органы;

е) защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных - работников Учреждения;

ж) предоставления работникам Учреждения персонализированных информационных сервисов для осуществления видов деятельности, предусмотренных Уставом и иными локальными правовыми актами Учреждения;

з) обеспечения пропускного и внутриобъектового режимов на объектах Учреждения;

и) формирования справочных материалов для внутреннего информационного обеспечения деятельности Учреждения, предусмотренной Уставом Учреждения;

к) исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

л) в иных целях, предусмотренных действующим законодательством

Российской Федерации.

2.4. Действия, совершаемые с персональными данными в Учреждении.

Учреждение осуществляет сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, предоставление, обезличивание, уничтожение персональных данных.

2.5. Согласие субъекта персональных данных на обработку его персональных данных в Учреждении.

Условием обработки персональных данных субъекта персональных данных является его письменное согласие.

Форма согласия на обработку персональных данных работника приведена в приложении № 2 к настоящему Положению.

Согласие на обработку персональных данных может быть отозвано субъектом персональных данных на основании письменного заявления в произвольной форме.

В случае если Учреждение на основании договора поручает обработку персональных данных третьей стороне, существенным условием договора является обязанность обеспечения третьей стороной конфиденциальности персональных данных и безопасности персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных. Также такой договор должен содержать перечень действий (операций) с персональными данными, цели и сроки обработки.

Форма заявления - согласия субъекта на передачу его персональных данных третьей стороне приведена в приложении № 3 к настоящему Положению.

Согласие физического лица не требуется в случаях:

а) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

б) обработка персональных данных необходима для исполнения договора, стороной, выгодоприобретателем или поручителем, по которому является субъект персональных данных;

в) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

г) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

д) обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем, при условии обязательного обезличивания персональных данных;

е) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

ж) осуществляется обработка персональных данных, подлежащих

опубликованию или обязательному раскрытию в соответствии с законодательством Российской Федерации.

3. Обработка персональных данных в Учреждении

3.1. Виды обработки персональных данных в Учреждении.

В Учреждении осуществляется:

а) автоматизированная обработка персональных данных в информационных системах персональных данных;

б) обработка персональных данных без использования средств автоматизации;

в) передача персональных данных другим операторам.

3.2. Обработка персональных данных без использования средств автоматизации.

3.2.1. Для каждой категории субъектов персональных данных, обрабатываемых без использования средств автоматизации в Учреждении, определяются отдельные места хранения персональных данных (материальных носителей) в запирающихся на ключ помещениях, в металлических несгораемых шкафах (сейфах), иных шкафах, имеющих запираемые блок-секции. Ключи от этих помещений (шкафов) должны храниться у лиц, ответственных за обработку персональных данных данной категории субъектов персональных данных. Запрещается хранение носителей с персональными данными на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам. Запрещается вынос носителей с персональными данными из служебных помещений для работы с ними вне Учреждения.

3.2.2. Перечень лиц, ответственных за обработку персональных данных в Учреждении, осуществляющих обработку персональных данных или имеющих к ним доступ утверждается приказом Учреждения.

3.2.3. Персональные данные субъектов персональных данных, обрабатываемые без использования средств автоматизации в Учреждении (материальные носители), обработка которых осуществляется в различных целях, должны храниться раздельно.

3.2.4. При хранении материальных носителей в Учреждении должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

3.3. Автоматизированная обработка персональных данных.

3.3.1. Автоматизированная обработка персональных данных в Учреждении осуществляется в информационных системах персональных данных.

3.3.2. Ответственные за обработку персональных данных в информационной системе персональных данных, пользователи и администратор должны быть ознакомлены со своими должностными инструкциями под роспись.

3.4. Порядок получения персональных данных.

3.4.1. Учреждение получает сведения о персональных данных субъектов персональных данных из следующих документов:

а) паспорт или иной документ, удостоверяющий личность;

б) трудовая книжка;

в) страховое свидетельство государственного пенсионного страхования;

г) свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;

д) документы воинского учета, содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;

е) документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащий сведения об образовании, профессии;

ж) анкета, заполняемая при приеме на работу, поступлении на обучение (в том числе при подаче заявлений на конкурс при поступлении или занятии должностей, предполагающих конкурсный отбор);

з) иные документы и сведения, предоставляемые субъектом персональных данных при приеме на работу, а также в процессе работы и обучения.

3.4.2. Субъект персональных данных обязан предоставлять Учреждению достоверные сведения о себе. Учреждение имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству Российской Федерации.

3.4.3. Все персональные данные субъекта персональных данных Учреждение получает непосредственно у указанных субъектов.

3.5.Порядок передачи персональных данных.

3.5.1. При передаче персональных данных работники Учреждения должны соблюдать следующие требования:

а) не сообщать персональные данные субъекта в коммерческих целях. Обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи не допускается.

б) осуществлять передачу персональных данных субъектов в пределах Учреждения в соответствии с настоящим Положением, локальными нормативными актами и должностными инструкциями.

в) разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения должностных обязанностей.

г) передавать персональные данные субъекта представителям субъекта в порядке, установленном законодательством и локальными нормативными актами и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

3.5.2. Форма журнала учета передачи персональных данных приведена в Приложении № 4 к настоящему Положению.

Ответственными за ведение журнала учета передачи персональных данных, является специалист по кадрам.

3.5.3. Учреждение не осуществляет трансграничную передачу персональных данных.

4. Обеспечение прав субъектов персональных данных при обработке их персональных данных в Учреждении

4.1. Права субъектов персональных данных.

4.1.1. Субъекты персональных данных имеют право на:

а) полную информацию об их персональных данных, обрабатываемых в Учреждении;

б) доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;

в) уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

г) отзыв согласия на обработку персональных данных;

д) принятие предусмотренных законом мер по защите своих прав;

е) обжалование действия или бездействия Учреждения, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;

з) осуществление иных прав, предусмотренных законодательством Российской Федерации.

4.2. Рассмотрение запросов на получение персональных данных субъектов.

4.2.1. Доступ к своим персональным данным предоставляется субъекту персональных данных или его законному представителю лицом, ответственным за обработку персональных данных, при обращении субъекта персональных данных (законного представителя). В качестве формы обращения субъекта персональных данных используется служебная записка на имя начальника Учреждения, собственноручно подписанная субъектом (законным представителем), содержащая номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе.

4.2.2. Сведения о наличии персональных данных должны быть представлены субъекту персональных данных пользователем ИСПДн в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных.

4.2.3. Субъект персональных данных имеет право на получение следующих сведений от пользователя ИСПДн:

а) подтверждение факта обработки персональных данных оператором;

б) правовые основания и цели обработки персональных данных;

в) цели и применяемые оператором способы обработки персональных данных;

г) сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального законодательства Российской Федерации;

д) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством Российской Федерации;

е) сроки обработки персональных данных, в том числе сроки их хранения;

ж) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

з) наименование и юридический адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

и) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами Российской Федерации.

4.2.4. Внесение изменений или уточнение персональных данных субъекта персональных данных пользователем ИСПДн должны быть выполнены в течение семи рабочих дней со дня предоставления таких сведений.

4.3. Порядок обеспечения конфиденциальности при обработке персональных данных.

4.3.1. Должностным лицам Учреждения, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных.

4.3.2. Без согласования с руководителем структурного подразделения Учреждения (филиалы, отделы) формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих персональные данные, запрещается.

4.3.3. Должностные лица Учреждения, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, указанных в согласии на обработку и передачу персональных данных субъектом персональных данных.

4.3.4. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством Российской Федерации, при заполнении согласия на передачу персональных данных третьей стороне, в соответствии с должностными инструкциями и иными локальными нормативными актами Учреждения.

4.3.5. Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом Учреждения на основании письменного или устного поручения руководителя структурного подразделения Учреждения.

4.3.6. Передача сведений и документов, содержащих персональные данные, оформляется путем внесения записи в Журнал учета передачи персональных данных.

4.3.7. Запрещается передача персональных данных по телефону, факсу,

электронной почте за исключением случаев, установленных законодательством Российской Федерации и действующими в Учреждении локальными правовыми актами.

4.3.8. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

4.3.9. Должностные лица Учреждения, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и (или) начальнику Учреждения обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостаче носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

4.3.10. Должностные лица Учреждения, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

5. Обязанности Учреждения как оператора

5.1. Меры, осуществляемые в Учреждении для обеспечения выполнения обязанностей оператора.

Меры по обеспечению выполнения Учреждения обязанностей оператора, предусмотренных законодательством Российской Федерации в области персональных данных, включают:

а) назначение лиц, ответственных за обработку персональных данных в Учреждении;

б) принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;

в) организацию обучения и проведение методической работы с работниками Учреждения, осуществляющими обработку персональных данных. Форма дополнительного соглашения к трудовому договору для работников, принимающих участие в обработке персональных данных, приведена в Приложении № 5 к настоящему Положению;

г) получение согласий субъектов персональных данных на обработку их персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;

д) обособление персональных данных, обрабатываемых без использования средств автоматизации, от иной информации, в частности путем их фиксации на отдельных материальных носителях персональных данных, в специальных разделах;

е) обеспечение раздельного хранения персональных данных и их

материальных носителей, обработка которых осуществляется в разных целях и которые содержат разные категории персональных данных;

ж) установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям и сетям Интернет без применения установленных в Учреждении мер по обеспечению безопасности персональных данных (за исключением общедоступных и (или) обезличенных персональных данных);

и) хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним. Форма журнала учета съемных носителей информации, содержащих персональных данных, утверждается приказом Учреждения.

к) ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации. Порядок доступа в помещения, где происходит обработка персональных данных, в рабочее и нерабочее время, а также в нештатных ситуациях осуществляется в соответствии с утвержденными приказом Учреждения Правилами доступа в помещения федерального бюджетного учреждения Волгоградская лаборатория судебной экспертизы Министерства юстиции Российской Федерации, где размещены и хранятся используемые средства криптографической защиты информации.

л) осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящему Положению, локальным нормативным актам Учреждения;

м) ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации и локальных нормативных актов Учреждения в области персональных данных, в том числе с требованиями к защите персональных данных, и обучение указанных работников;

н) опубликование или обеспечение неограниченного доступа к настоящему Положению иным образом;

о) прекращение обработки и уничтожение персональных данных в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

п) иные меры, предусмотренные законодательством Российской Федерации в области персональных данных.

5.2. Меры, осуществляемые в Учреждении по обеспечению безопасности персональных данных при их автоматизированной обработке.

5.2.1. Автоматизированная обработка персональных данных (ПДн) в Учреждении осуществляется в информационной системе персональных данных (ИСПДн) «1С: Предприятие: Зарплата и кадры бюджетного учреждения»

5.2.2. Обеспечение безопасности ПДн при их автоматизированной обработке в Учреждении осуществляется применением организационных и технических мер с

целью предотвращения неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, разглашения, а также иных неправомерных действий в отношении ПДн.

5.2.3. Для обеспечения безопасности ПДн при их автоматизированной обработке в Учреждении осуществляются следующие организационные меры:

а) ограничение доступа работников Учреждения к средствам обработки и защиты ПДн ИСПДн Учреждения;

в) обеспечение невозможности визуального просмотра ПДн, отображаемых на экранах мониторов и зафиксированных на бумажных носителях ПДн, лицами, не имеющими прав доступа к этим ПДн;

г) принятие работниками Учреждения – пользователями и администратором информационных систем персональных данных обязательства не разглашать ПДн, ставшие им известными при выполнении ими своих должностных обязанностей;

д) строгое соблюдение пользователями и администратором информационных систем персональных данных;

е) обеспечение условий хранения отчуждаемых и съемных носителей ПДн всех ИСПДн, исключающих возможность их утраты, несанкционированного доступа к ним и несанкционированного воздействия на них;

з) восстановление ПДн, целостность которых была нарушена в результате несанкционированных и (или) непреднамеренных воздействий на них или их носитель;

и) установление правил доступа к ПДн, обрабатываемым во всех ИСПДн, персонала ИСПДн;

к) учет всех ПДн, обрабатываемых во всех ИСПДн и передаваемых другим операторам (органам государственной власти и юридическим лицам);

л) контроль за принимаемыми мерами по обеспечению безопасности ПДн при их обработке в ИСПДн.

5.2.4. Для обеспечения безопасности ПДн при их автоматизированной обработке в Учреждении осуществляются следующие технические меры:

а) функционирование в составе всех ИСПДн средств защиты информации (СрЗИ), функционально объединенных в систему защиты информации (СЗИ) ИСПДн;

б) использование для обеспечения безопасности ПДн во всех ИСПДн сертифицированных по требованиям безопасности информации СрЗИ;

в) использование в составе СЗИ ИСПДн СрЗИ, осуществляющих идентификацию и аутентификацию пользователей и администратора информационных систем персональных данных;

г) оборудование помещений, в которых размещаются компоненты всех ИСПДн, а также хранятся отчуждаемые и съемные носители ПДн, техническими средствами охранной и пожарной сигнализации, средствами физической защиты информации;

д) использование специальных средств гарантированного уничтожения Пдн, подлежащих уничтожению в соответствии с законодательством Российской Федерации.

5.3. Меры, осуществляемые в Учреждении, по обеспечению безопасности персональных данных при их обработке без использования средств автоматизации.

5.3.1. Обработка персональных данных без использования средств автоматизации осуществляется в Учреждении в бухгалтерии и специалистом по кадрам.

5.3.2. Обеспечение безопасности ПДн при их обработке без использования средств автоматизации в Учреждении осуществляется применением организационных и технических мер с целями предотвращения неправомерного доступа к ним и их носителям, разглашения их, обеспечения их целостности и сохранности их носителей.

5.3.3. Для обеспечения безопасности ПДн при их обработке без использования средств автоматизации в Учреждении осуществляются следующие организационные меры:

а) функционирование организационной структуры системы обработки персональных данных Учреждения;

б) обеспечение возможности определения места хранения ПДн на носителях ПДн для каждой категории ПДн и субъектов ПДн;

в) установление перечня работников Учреждения, осуществляющих обработку ПДн или имеющих право доступа к ним и (или) их носителям;

г) раздельное хранение ПДн на носителях ПДн, обработка которых осуществляется в различных целях;

д) принятие работниками Учреждения, осуществляющими обработку ПДн или имеющими право доступа к ним или их носителям, обязательства не разглашать ПДн, ставшие им известными при выполнении своих должностных обязанностей;

е) запрет на несанкционированное копирование, уничтожение и изменение ПДн.

5.3.4. Для обеспечения безопасности ПДн при их обработке без использования средств автоматизации в Учреждении осуществляется следующие технические меры:

а) оборудование помещений, где осуществляется хранение носителей ПДн, техническими средствами охранной и пожарной сигнализации (при необходимости);

б) использование средств физической защиты информации (средств и систем контроля и управления доступом в помещения, защитных ограждений оконных проемов);

г) использованием специальных технических средств гарантированного уничтожения носителей ПДн, ПДн на которых подлежат уничтожению в соответствии с законодательством Российской Федерации и локальными правовыми актами Университета.

5.4. Меры, осуществляемые в Учреждении по устранению нарушений законодательства, допущенных при обработке персональных данных.

5.4.1. Работники Учреждения, непосредственно осуществляющие обработку ПДн, могут случайно или преднамеренно допускать следующие нарушения законодательства Российской Федерации:

а) осуществлять неправомерную обработку ПДн;

б) осуществлять обработку неточных ПДн;

в) не прекращать обработку ПДн в случае достижения цели обработки;

г) не прекращать обработку ПДн в случае отзыва субъектом ПДн согласия на обработку его Пдн.

5.4.2. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта ПДн или его представителя либо уполномоченного органа по защите прав субъектов персональных данных ответственный за организацию обработки этих ПДн должен поручить администратору информационной системы персональных данных (если осуществлялась автоматизированная обработка этих ПДн) или работнику Учреждения, неправомерно осуществлявшему обработку Пдн, но имевшего право обрабатывать эти Пдн (если осуществлялась обработка без использования средств автоматизации) осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки.

5.4.3. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных руководитель соответствующего структурного подразделения Учреждения должен поручить администратору информационной системы персональных данных (если осуществлялась автоматизированная обработка этих ПДн) или работнику Учреждения, которому поручено осуществлять неавтоматизированную обработку ПДн этого субъекта, осуществить блокирование этих неточных ПДн с момента такого обращения или получения указанного запроса на период проверки, которую должен организовать вышеназванный руководитель структурного подразделения Учреждения, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

5.4.4. В случае подтверждения факта неточности ПДн руководитель соответствующего структурного подразделения Учреждения на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан обеспечить их уточнение в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных;

5.4.5. В случае выявления неправомерной обработки ПДн, осуществляемой ответственным за организацию обработки этих ПДн, должен поручить администратору информационной системы персональных данных (если осуществлялась автоматизированная обработка этих ПДн) или работнику Учреждения, неправомерно осуществлявшему обработку Пдн, но имевшего право обрабатывать эти Пдн (если осуществлялась обработка без использования средств автоматизации) в срок, не превышающий трех рабочих дней с даты этого выявления, прекратить неправомерную обработку персональных данных.

Если по результатам проверки выявлена невозможность обеспечить правомерную обработку ПДн, руководитель соответствующего структурного подразделения Учреждения обязан в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, организовать уничтожение этих

ПДн.

Об устранении допущенных нарушений или об уничтожении ПДн руководитель соответствующего структурного подразделения Учреждения, организовавший проверку возможности правомерной обработки ПДн, обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также орган.

5.4.6. В случае достижения цели обработки ПДн руководитель соответствующего структурного подразделения Учреждения обязан организовывать прекращение обработки ПДн и уничтожение ПДн в срок, не превышающий тридцать дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДН либо если Учреждение не вправе осуществлять обработку ПДН без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

5.4.7. В случае отзыва субъектом ПДн согласия на обработку его ПДн руководитель соответствующего структурного подразделения Учреждения обязан обеспечить прекращение такой обработки и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, обеспечить их уничтожение в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между Учреждением и субъектом ПДн либо если Учреждение не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

В случае отсутствия возможности уничтожения ПДн в течение указанного в пунктах 5.4.5 – 5.4.7 Положения срока, руководитель соответствующего структурного подразделения Учреждения должен организовать блокирование таких ПДн и обеспечить их уничтожение в установленном порядке в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.5. Меры, осуществляемые в Учреждении по уведомлению об обработке ПДн.

5.5.1. Учреждение до начала обработки ПДн уведомляет уполномоченный орган по защите прав субъектов ПДн (далее – Уполномоченный орган) о своем намерении осуществлять обработку ПДн.

5.5.2. Уведомление готовят ответственные за обработку ПДн в Учреждении.

5.5.3. Уведомление направляется в письменной форме и содержит следующие сведения:

а) наименование, адрес Учреждения;

б) цели обработки персональных данных;

в) категории обрабатываемых персональных данных;

г) категории субъектов, персональные данные которых обрабатываются;

д) правовое основание обработки персональных данных;

е) перечень действий, осуществляемых с персональными данными, общее описание используемых в Учреждении способов обработки персональных данных;

ж) описание мер, которые Учреждение осуществляет по обеспечению безопасности персональных данных, в том числе сведения об используемых шифровальных (криптографических) средствах и наименовании этих средств;

з) дата начала обработки персональных данных;

и) срок или условие прекращения обработки персональных данных;

к) сведения о наличии или отсутствии трансграничной передачи персональных данных в процессе их обработки;

л) сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

5.5.4. Учреждение вправе осуществлять без уведомления Уполномоченного органа обработку персональных данных:

а) обрабатываемых в соответствии с трудовым законодательством;

б) полученных Учреждением в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Учреждением исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;

в) сделанных субъектом персональных данных общедоступными;

г) включающих в себя только фамилии, имена и отчества субъектов персональных данных;

д) необходимых в целях однократного пропуска субъекта персональных данных в здание (помещение) Учреждения;

е) включенных в информационные системы персональных данных, имеющие в соответствии с Федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

ж) обрабатываемых без использования средств автоматизации в соответствии с Федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных;

з) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

5.5.5. В случае изменения сведений, указанных в пункте 5.6.3 настоящего Положения, Учреждение уведомляет об изменениях Уполномоченный орган в

течение десяти рабочих дней с даты возникновения таких изменений. Уведомление об изменениях готовят должностные лица, указанные в п. 5.6.2 настоящего Положения.

6. Организационная структура системы обработки персональных данных Учреждения

6.1. Должностные лица, составляющие организационную структуру системы обработки персональных данных Учреждения.

6.1.1. Организационную структуру системы обработки персональных данных Учреждения составляют:

а) Ответственный за обеспечение безопасности персональных данных в информационной системе Учреждения (далее - Ответственный);

б) должностные лица, имеющие доступ к персональным данным обрабатываемым в информационной системе, ответственные за обработку персональных данных в Учреждении (далее – Ответственные за обработку);

в) администратор информационных систем персональных данных Учреждения (далее - Администратор);

г) руководители структурных подразделений, в которых осуществляется обработка ПДн любого вида (далее – Руководители структурных подразделений);

д) работники Учреждения, правомерно осуществляющие обработку ПДн без использования средств автоматизации или имеющие право доступа к таким ПДн или их носителям (далее - Обработчики ПДн).

6.1.2. Общее руководство организацией обработки ПДн в Учреждении осуществляет Ответственный, которым по должности является заместителем начальника Учреждения.

6.1.3. Непосредственную обработку ПДн в Учреждении осуществляют Ответственные за обработку, назначаемые приказом Учреждения по представлению Ответственного.

6.1.4. Администратор обеспечивает функционирование ИСПДн Учреждения.

6.1.5. Руководители структурных подразделений осуществляют контроль за обработкой ПДн в возглавляемых ими структурных подразделениях Учреждения, готовят представления начальнику Учреждения о назначении Ответственных за обработку (при условии эксплуатации в их структурных подразделениях ИСПДн) и (или) представления о назначении Обработчиков ПДн (при условии обработки в их структурных подразделениях ПДн без использования средств автоматизации).

6.1.6. Обработчики ПДн осуществляют обработку ПДн без использования средств автоматизации и назначаются приказом Учреждения по представлению руководителей структурных подразделений, в которых осуществляется обработка ПДн без использования средств автоматизации.

6.2. Ответственность должностных лиц, составляющих организационную структуру системы обработки персональных данных.

Должностные лица, составляющие организационную структуру системы обработки персональных данных Учреждения и перечисленные в пункте 6.1.1 настоящего Положения несут за нарушение законодательства Российской

Федерации в области персональных данных, локальных правовых актов Учреждения и настоящего положения уголовную, административную и дисциплинарную ответственность в соответствии с Уголовным кодексом Российской Федерации, Кодексом Российской Федерации об административных правонарушениях, Трудовым кодексом Российской Федерации.

7. Организация контроля за обработкой и защитой персональных данных в Учреждении

7.1. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства.

7.1.1. Контроль за соблюдением структурными подразделениями Учреждения законодательства Российской Федерации и локальных правовых актов Учреждения в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных в структурных подразделениях Учреждения законодательству Российской Федерации и локальным правовым актам Учреждения в области персональных данных, в том числе требованиям к защите персональных данных, а также принятых мер, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.

7.1.2. Внутренний контроль за соблюдением структурными подразделениями Учреждения законодательства Российской Федерации и локальных правовых актов Учреждения в области персональных данных, в том числе требований к защите персональных данных, а также внутренний контроль соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, настоящему Положению, локальным правовым актам Учреждения обеспечивается ответственным за обеспечение безопасности персональных данных в информационной системе Учреждения.

7.1.3. Персональная ответственность за соблюдение требований законодательства Российской Федерации и локальных правовых актов Учреждения в области персональных данных в структурном подразделении Учреждения, а также за обеспечение безопасности персональных данных в указанных подразделениях Учреждения возлагается на их руководителей.

7.2. Организация контроля за автоматизированной обработкой персональных данных.

7.2.1. Контроль за автоматизированной обработкой персональных данных субъектов персональных данных в ИСПДн Учреждения осуществляется администратором ИСПДн.

7.2.2. При обнаружении несанкционированного доступа к персональным данным субъектов персональных данных в ИСПДн Учреждения, утечки персональных данных субъектов, обрабатываемых в ИСПДн Учреждения, а также

нарушении установленного режима работы системы защиты информации ИСПДн, администратор ИСПДн обязан прекратить эксплуатацию ИСПДн и доложить о случившемся руководителю структурного подразделения и администратору ИСПДн, а также начальнику Учреждения.

7.2.3. Администратор ИСПДн обязан принять меры по защите персональных данных субъектов, обрабатываемых в ИСПДн, а в случае невозможности выполнения своих обязательств - доложить ответственному за обеспечение безопасности персональных данных в информационной системе Учреждения.

7.2.4. На основании полученной информации, ответственный за обеспечение безопасности персональных данных в информационной системе Учреждения с уведомлением начальника Учреждения имеет право приостановить эксплуатацию ИСПДн до выяснения обстоятельств и устранения причин выявленных нарушений безопасности при обработке персональных данных субъектов персональных данных в ИСПДн Учреждения.

7.3. Организация защиты персональных данных при их автоматизированной обработке.

7.3.1. Для автоматизированной обработки персональных данных в Учреждении может быть создана ИСПДн.

7.3.2. После ввода ИСПДн в эксплуатацию Администратор создает учетные записи и настраивает права доступа к информации всех ее пользователей. Администратор обеспечивает функционирование средств защиты информации в ИСПДн и контроль их настроек.

7.4. Организация защиты персональных данных при их обработке без использования средств автоматизации.

Организация защиты персональных данных при их обработке без использования средств автоматизации осуществляется Ответственным за обеспечение безопасности персональных данных в информационной системе Учреждения.

7.5. Организация уничтожения персональных данных.

7.5.1. Уничтожение персональных данных осуществляется:

а) по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом - в течение 30 дней;

б) при предоставлении субъектом персональных данных сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки - в течение 7 дней;

в) если невозможно обеспечить правомерность обработки персональных данных - в течение 10 дней;

г) в случае отзыва субъектом персональных данных согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных - в течение 30 дней.

7.5.2. При невозможности уничтожения персональных данных в сроки, определенные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» для случаев, когда невозможно обеспечить правомерность обработки персональных данных, при достижении целей обработки персональных данных, а

также при отзыве субъектом согласия на обработку персональных данных, если сохранение персональных данных более не требуется для целей обработки персональных данных, Учреждение осуществляет блокирование персональных данных и уничтожает персональные данные в течение 6 месяцев, если иной срок не установлен законодательством Российской Федерации.

7.5.3. Уничтожение персональных данных в Учреждении производится способом, исключающим возможность восстановления этих персональных данных на материальном носителе.

7.5.4. Уничтожение носителей персональных данных в Учреждении производится комиссией, назначаемой приказом Учреждения. Комиссия составляет акт об уничтожении персональных данных, который утверждает начальник Учреждения. Форма акта об уничтожении персональных данных согласно приложению № 6 к настоящему Положению.