УТВЕРЖДАЮ

Директор МАОУ «СОШ № 91 г. Челябинска»

_____ Л.А. Иванова

«20» октября 2017 г.

ПОЛОЖЕНИЕ
по организации и порядку проведения работ по обеспечению безопасности персональных данных работников МАОУ «СОШ № 91 г. Челябинска»

2017 г.

1 Общие положения

1.1 Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом Российской Федерации, Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой персональных данных и определяет порядок организации и проведения работ по обеспечению безопасности персональных данных работников МАОУ «СОШ № 91 г. Челябинска» (далее – учреждение).

1.2 Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных работников учреждения с использованием средств автоматизации или без использования таких средств.

1.3 Настоящее Положение и изменения к нему утверждаются руководителем учреждения и вводятся приказом.

1.4 Все работники учреждения должны быть ознакомлены под роспись с Положением и изменениями к нему.

1.5 Обработка персональных данных работников учреждения осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия работникам учреждения в трудоустройстве, выполнении ими своих функциональных обязанностей, в получении образования и продвижении по службе, предоставления им предусмотренных законодательством Российской Федерации и внутренними нормативными актами учреждения льгот, обеспечения личной безопасности работников, контроля качества и количества выполняемой работы и обеспечения сохранности имущества.

1.6 Методическое руководство и контроль за соблюдением требований по обработке персональных данных, контроль за соблюдением прав и свобод субъектов персональных данных возлагается на руководителя учреждения.

2 Основные понятия

Работники - лица, имеющие трудовые отношения с Учреждением, либо кандидаты на вакантную должность, вступившие с Учреждением в отношения по поводу приема на работу.

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

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), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

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

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

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

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.ъ

3 Принципы обработки персональных данных

3.1 Обработка персональных данных должна осуществляться на основе принципов:

– законности целей и способов обработки персональных данных и добросовестности;

– соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

– соответствия объема и характера обрабатываемых персональных данных, способов обработки целям обработки персональных данных;

– достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

– недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

– обеспечения точности персональных данных, их достаточности, актуальность по отношению к целям обработки персональных данных;

– осуществления хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

3.2 Запрещается получать и обрабатывать специальные категории персональных данных, в частности персональные данные о политических, религиозных и иных убеждениях, состоянии здоровья, частной жизни, членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

3.3 При принятии решений относительно субъекта ПДн на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей.

3.4 Защита персональных данных субъектов ПДн от неправомерного их использования или утраты обеспечивается за счет средств учреждения. Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационной системе оценивается при проведении государственного контроля и надзора и периодического внутреннего контроля.

4 Состав и субъекты персональных данных

4.1 К субъектам персональных данных относятся:

– работники учреждения, включая совместителей, а также лица, выполняющие работы по договорам гражданско-правового характера;

– студенты, проходящие практику;

4.2 Перечень персональных данных, обрабатываемых в учреждении, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами учреждения с учетом целей обработки персональных данных.

5 Порядок обработки персональных данных работников

5.1 Получение персональных данных

5.1.1 Учреждение получает сведения о персональных данных субъектов персональных данных при поступлении на работу в учреждение из следующих документов:

– паспорт или иной документ, удостоверяющий личность;

– трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

– страховое свидетельство государственного пенсионного страхования;

– документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;

– документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

– свидетельство о присвоении ИНН (при его наличии у работника);

– анкета, заполняемая при приеме на работу;

– санитарная книжка; медицинская справка о прохождении медицинского осмотра;

– иные документы и сведения, предоставляемые субъектом персональных данных при приеме на работу, а также в процессе трудовой деятельности.

Субъект персональных данных обязан представлять учреждению достоверные сведения о себе. Учреждение имеет право проверять достоверность указанных сведений в порядке, не противоречащим законодательству РФ. Субъект персональных данных обязан своевременно, в срок, не превышающий одного месяца, сообщать учреждению об изменении своих персональных данных.

5.1.2 Информация, представляемая работником при поступлении на работу в учреждении, должна иметь документальную форму. При заключении трудового договора лицо, поступающее на работу, предъявляет работодателю документы описанные в ст. 65 Трудового кодекса Российской Федерации.

5.1.3 При оформлении работника в учреждение уполномоченным работником заполняется унифицированная форма Т-2 «Личная карточка работника», которая отражает данные работника в соответствии с трудовым законодательством.

5.1.4 Все персональные данные работника учреждение получает у него самого. Сотрудник, ответственный за документационное обеспечение кадровой деятельности, принимает от субъекта документы, проверяет их полноту и правильность указываемых сведений.

5.1.5 Если персональные данные работника возможно получить только у третьей стороны, то работник уведомляется об этом заранее. У работника берется его письменное согласие. Учреждение сообщает работнику о целях, предполагаемых источниках и способах получения его персональных данных.

5.2 Хранение персональных данных

5.2.1 Документы, содержащие персональные данные работника составляют его личное дело. Личное дело ведется на протяжении всей трудовой деятельности работников. Изменения, вносимые в личное дело, подтверждаются соответствующими документами.

5.2.2 Личное дело хранится уполномоченным лицом на бумажных носителях.

5.2.3 Для хранения персональных данных используются шкафы, которые запираются на ключ. Ключ от шкафов, в которых хранятся сведения о работниках учреждения, находится у руководителя учреждения, а при его отсутствии — у иного уполномоченного лица.

5.2.4 Учреждение осуществляет обработку только тех персональных данных работника о состоянии здоровья, которые относятся к вопросу о возможности выполнения работником трудовой функции (на бумажных носителях).

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Обработка указанных персональных данных работников работодателем возможна только с их согласия либо без их согласия в следующих случаях:

– персональные данные являются общедоступными;

– персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

– по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

5.2.5 В случаях, предусмотренных законодательством, обработка специальных категорий персональных данных и сведений, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрических персональных данных) может осуществляться в учреждении только с его письменного согласия.

5.2.6 Персональные данные работников могут проходить дальнейшую обработку и передаваться на хранение в электронном виде - локальной компьютерной сети и компьютерной программе.

5.2.7 При обработке персональных данных руководитель учреждением вправе определять способы обработки, документирования, хранения и защиты персональных данных на базе современных информационных технологий.

5.2.8 После прекращения юридических отношений с субъектом персональных данных (увольнения работника, расторжения договора и т.п.) документы, содержащие его персональные данные, хранятся в учреждении в течение сроков, установленных архивным и иным законодательством РФ. Режим конфиденциальности персональных данных работников снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии учреждения, если иное не определено законом.

5.3 Доступ к персональным данным

5.3.1 Круг лиц, допущенных к работе (получению, обработке, передаче и хранению персональных данных субъекта) с документами, содержащими персональные данные субъектов, определяется руководителем учреждением. Уполномоченные лица имеют право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций.

5.3.2 Право доступа к персональным данным работников учреждения утверждается приказом по организации.

5.3.3 Работа по обработке персональных данных возлагается на работников учреждения, назначенных ответственными за обеспечение безопасности ПДн, которые действуют на основании инструкции.

5.3.4 Разрешительная система доступа пользователей к информационным ресурсам оформляется лицом, ответственным за обеспечение безопасности ПДн, в виде матриц доступа, утверждаемых руководителем учреждения, и реализуется с помощью средств защиты от несанкционированного доступа. Матрицы доступа отражает полномочия пользователей по выполнению конкретных действий в отношении информационных ресурсов ИСПДн (чтение, запись, корректировка, удаление).

5.3.5 Внешний доступ со стороны третьих лиц к персональным данным субъекта осуществляется с его письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта или других лиц, и иных

случаев, установленных законодательством.

5.4 Передача персональных данных

5.4.1 Передача персональных данных работника осуществляется как в пределах учреждения в соответствии с нормативными актами, с которыми работник должен быть ознакомлен под роспись, так и вне учреждения (по сети Интернет) в установленном порядке.

5.4.2 В соответствии с законодательством учреждением осуществляется передача персональных данных в следующие государственные органы:

- Инспекция федеральной налоговой службы;
- Пенсионный фонд России;
- Фонд социального медицинского страхования;
- Банк;
- Контрольно-надзорные органы.

5.4.3 При передаче персональных данных работника запрещается:

- 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 Трудовым кодексом или иными федеральными законами;
- сообщать персональные данные работника в коммерческих целях без его письменного согласия.

5.4.4 При передаче персональных данных работники учреждения предупреждают лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим конфиденциальности.

5.4.5 Передача персональных данных работника представителям работников осуществляется в порядке, установленном Трудовым кодексом и иными федеральными законами. Передаваемая информация ограничивается только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

5.4.6 Передача и предоставление ПДн законным пользователям осуществляется способом, не допускающим возможность несанкционированного доступа к ним посторонних лиц.

5.4.7 Запрещается предоставлять персональные данные работника учреждения лицам, не уполномоченным федеральным законом на получение персональных данных, либо при отсутствии письменного согласия работника на предоставление его персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

5.4.8 Трансграничная передача персональных данных запрещена.

5.5 Уточнение, изменение, блокирование персональных данных

5.5.1 В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченными работниками учреждения вносятся в них необходимые изменения.

5.5.2 В случае выявления неточных персональных данных или неправомерной обработки 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 учреждение осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, с момента такого обращения или получения указанного запроса на период проверки. В случае подтверждения факта неточности персональных данных учреждение на основании соответствующих документов уточняет персональные данные в течении семи дней и снимает их блокирование.

5.6 Уничтожение персональных данных

5.6.1 В срок, не превышающий семи рабочих дней со дня представления субъектом

персональных данных или его представителем сведений, подтверждающих, что его персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные работники учреждения уничтожают такие персональные данные.

5.6.2 В случае выявления неправомерной обработки персональных данных, учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно, учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

5.6.3 В случае достижения цели обработки персональных данных учреждение прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

5.6.4 В случае отзыва субъектом персональных данных согласия на обработку его персональных данных учреждение прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные 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 персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных федеральными законами.

6 Права субъектов персональных данных

6.1 Субъекты персональных данных имеют право:

– получать полную информацию об их персональных данных и обработке этих данных;

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

– определять своих представителей для защиты своих персональных данных;

– получать свободный бесплатный доступ к медицинской документации, отражающей состояние их здоровья, с помощью медицинского работника по их выбору;

– требовать 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;

– требовать об исключении или исправлении неверных, или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса 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;

– отозвать согласие на обработку своих персональных данных;

– 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;

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

– осуществление иных прав, предусмотренных законодательством Российской Федерации.

6.2 Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

6.3 Порядок обработки запросов субъектов персональных данных регламентируется «Правилами рассмотрения запросов субъектов персональных данных или их представителей».

6.4 Субъект персональных данных не должен отказываться от своих прав на сохранение и защиту охраняемой законом тайны.

7 Обязанности учреждения при обработке персональных данных

7.1 При сборе и обработке персональных данных уполномоченные работники учреждения обязаны предоставить субъекту персональных данных по его просьбе следующую информацию:

– подтверждение факта обработки персональных данных;

– правовые основания и цели обработки персональных данных;

– цели и применяемые способы обработки персональных данных;

– наименование и место нахождения оператора, 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 закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7.2 Если предоставление персональных данных является обязательным в соответствии с федеральным законом, уполномоченные работники учреждения обязаны разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

7.3 Если персональные данные получены не от субъекта персональных данных, уполномоченные работники учреждения, за исключением случаев, если персональные данные были предоставлены Учреждению на основании федерального закона или если персональные данные являются общедоступными, до начала обработки таких персональных данных обязаны предоставить субъекту персональных данных следующую информацию:

- наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- права субъекта персональных данных;
- источник получения персональных данных.

7.4 Учреждение обязано безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к соответствующему субъекту, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом сведений, подтверждающих, что персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели

обработки. О внесенных изменениях и предпринятых мерах Учреждение обязано уведомить соответствующего субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта были переданы.

8 Меры, направленные на обеспечение выполнения Оператором обязанностей, предусмотренных Федеральным законом «О персональных данных»

8.1 Учреждение при осуществлении обработки персональных данных:

– принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов учреждения в области персональных данных;

– принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

– назначает лицо, ответственное за организацию обработки персональных данных в учреждении;

– издает локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в учреждении;

– сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;

– прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;

– в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в учреждении проводятся периодические проверки условий обработки персональных данных;

– совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных.

8.2 Сотрудники учреждения, ответственные за хранение персональных данных, а также сотрудники учреждения, владеющие персональными данными в силу своих должностных обязанностей, подписывают Обязательство о конфиденциальности.

8.3 Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита информации, обрабатываемой техническими средствами, а также информации содержащаяся на носителях на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн.

8.4 Все магнитные, оптические и другие машинные носители ПДн подлежат обязательному учету. На носители информации наносится маркировка, позволяющая идентифицировать и организовать их учет. Машинные носители информации, в том числе с резервными копиями ПДн, регистрируются в журнале учета машинных носителей ПДн, в котором отражается:

– тип и емкость носителя;
– учетный номер носителя;
– место установки (использования) носителя;
– дата установки носителя;
– ответственное должностное лицо;
– сведения о списании носителя и уничтожении информации.

8.5. Пользователям запрещается использовать съемные носители информации за исключением случаев, когда использование съемных носителей необходимо в рамках должностных обязанностей.

8.6 Помещения, в которых хранятся персональные данные субъектов, оборудуются сейфами, надежными замками, противопожарной сигнализацией. В рабочее время при отсутствии работников помещения запираются на ключ. Проведение уборки помещений, в которых хранятся персональные данные, производится в присутствии соответствующих работников.

8.7 Работники учреждения, назначенные ответственными за обеспечение безопасности персональных данных, осуществляют ознакомление работников учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных.

8.8 Не реже одного раза в год проводится внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами учреждения.

8.9 В целях информационного обеспечения в учреждении создаются общедоступные источники персональных данных сотрудников (далее – Справочники), в которые включаются его фамилия, имя, отчество, сведения о занимаемой им должности, номер служебного телефона, иные персональные данные, предоставленные субъектом персональных данных.

8.10 Формирование, ведение и иные действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, содержащихся в Справочниках осуществляются подразделениями учреждения, ответственными за ведение каждого Справочника.

9 Правила работы с обезличенными данными

9.1 Обезличивание персональных данных в учреждении проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

9.2 При использовании процедуры обезличивания не допускается совместное хранение персональных данных и обезличенных данных.

9.3 Способы обезличивания при условии дальнейшей обработки персональных данных:

– замена части сведений идентификаторами;

– изменение состава или семантики – изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения, преобразования или удаления части сведений.

9.4 Решение о необходимости обезличивания персональных данных принимает руководитель учреждения.

9.5 Работники учреждения, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

9.6 Работники учреждения, непосредственно осуществляющие обработку персональных данных, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

9.7 Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

9.8 Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

9.9 При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

– парольной политики;

– антивирусной политики;

– правил работы со съемными носителями (если они используется);

– правил резервного копирования;
– правил доступа в помещения, где расположены элементы информационных систем.

9.10 При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
– правил хранения бумажных носителей;
– правил доступа к ним и в помещения, где они хранятся.

10 Ответственность за нарушение требований, регулирующих получение, обработку и хранение персональных данных сотрудника

10.1 Лица, виновные в нарушении требований, регулирующих получение, обработку и хранении персональных данных сотрудника несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

10.2 Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы:

– руководитель, разрешающий доступ сотрудника к персональным данным несет персональную ответственность за данное разрешение;

– каждый работник учреждения несет единоличную ответственность за сохранность носителей персональных данных и соблюдение конфиденциальности информации;

– работник учреждения, предоставивший работодателю подложные документы или заведомо ложные сведения о себе, либо своевременно не сообщивший об изменениях персональных данных, несет дисциплинарную ответственность, вплоть до увольнения.

10.3 Лица, виновные в нарушении условий использования средств защиты информации или нарушении режима защиты персональных данных, несут ответственность в соответствии с законодательством Российской Федерации.

10.4 Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом «О персональных данных», а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.