УТВЕРЖДЕНА
Приказом директор МКУ «ЕДДС Дзержинский»
от 30 марта 2018 г. № 30

ПОЛИТИКА

муниципального казенного учреждения «Единая дежурно-диспетчерская служба Дзержинский» в отношении обработки информации и защиты персональных данных

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 г. № 149 «Об информации, информационных технологиях и о защите информации», Федеральным Законом от 27.07.2006 г. № 152 «О персональных данных», Федеральным законом от 21.12.1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (с изменениями от 02.07.2013 г. № 158-ФЗ), Постановления Правительства Российской Федерации от 24.03.1997 г. № 334 «О Порядке сбора и обмена в Российской Федерации информацией в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера» (в ред. Постановления Правительства Российской Федерации от 10.09.2013 г. № 793), Федерального закона от 07.062017 г. № 110-ФЗ О внесении изменений в статью 66 Федерального закона «О связи» и статью 35 Закона Российской Федерации «О средствах массовой информации», Постановлением Правительства от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства от 05.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства от 03.11.1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» (с изменениями и дополнениями 2016 года), приказом ФСТЭК от 18.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом ФСТЭК от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК от 14.03.2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», Приказом Минкомсвязи России от 30.11.2015 г. № 484 «Об утверждении Правил применения оборудования центров обработки вызовов экстренных оперативных служб. Часть I. Правила применения оборудования центров обработки вызовов экстренных оперативных служб по единому номеру «112», Приказом Минкомсвязи России от 15.09.2015 г. № 349 «Об утверждении Правил применения оборудования узлов обслуживания вызовов экстренных оперативных служб», Приказом Минкомсвязи России от 01.12.2016 г. № 607 «Об утверждении Правил определения места

нахождения пользовательского оборудования (оконечного оборудования), с которого были осуществлены вызов или передача сообщения о происшествии по единому номеру вызова экстренных оперативных служб «112», и Порядка предоставления и объема информации, необходимой для обеспечения реагирования по вызову или сообщению о происшествии по единому номеру вызова экстренных оперативных служб «112», другими нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой персональных данных, и определяет политику обработки персональных данных, порядок организации и проведения работ по обеспечению безопасности персональных данных в муниципальном казенном учреждении «Единая дежурно-диспетчерская служба Дзержинский» (далее – Учреждение, ЕДДС).

1.2. ЕДДС является оператором, самостоятельно организующим и осуществляющим обработку персональных данных субъектов персональных данных (далее – персональные данные), а также определяющим цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.3. Настоящей Политикой определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных в Учреждении с использованием средств автоматизации или без использования таких средств.

1.4. Работники ЕДДС, осуществляющие обработку персональных данных, должны быть ознакомлены под личную подпись с настоящей Политикой и изменениями к ней.

1.5. Методическое руководство и контроль за соблюдением требований по обработке персональных данных, контроль за соблюдением прав и свобод субъектов персональных данных возлагается на ответственного за организацию обработки персональных данных в Учреждении.

2. Основные понятия

Персональные данные – любая информация, относящаяся к прямо или косвенно определённому, 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. В настоящей Политике понятие «оператор» применяется к учреждению.

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.

Обработка персональных данных включает в себя:

- сбор;
- запись;
- систематизацию;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передачу (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

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.

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

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

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределённому кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц.

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

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.

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.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных осуществляется на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- согласие на обработку персональных данных (в случаях, прямо не предусмотренных законодательством Российской Федерации, но соответствующих полномочиям оператора);
- соответствия целей обработки персональных данных целям, заранее определённым и заявленным при сборе персональных данных;
- соответствия объёма 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 обрабатывать и приобщать к личному делу гражданского служащего не установленные Федеральными законами персональные данные о его политических, религиозных и иных убеждениях и частной жизни, о членстве в общественных объединениях, в том числе в профессиональных союзах.

3.3. При принятии решений, затрагивающих интересы субъекта персональных данных, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей.

3.4. Защита персональных данных от неправомерного их использования или утраты обеспечивается за счёт 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.

3.5. При осуществлении хранения персональных данных оператор персональных данных обязан использовать базы данных, находящиеся на территории Российской Федерации.

4. Цели обработки персональных данных

4.1. Для каждой категории субъектов персональных данных определены цели обработки их персональных данных.

4.2. Целями обработки персональных в Учреждении являются исполнение правовых актов, регламентирующих деятельность оператора, целей фактически осуществляемой оператором деятельности, а также деятельности, которая предусмотрена учредительными документами оператора, и конкретных рабочих процессов оператора в конкретных информационных системах персональных данных (по структурным подразделениям оператора и их процедурам в отношении определенных категорий субъектов персональных данных).

4.3. Целями обработки персональных данных работников Учреждения являются:

– ведение кадрового делопроизводства;

– начисление и выплата заработной платы, вознаграждений, премирования, материальной помощи;

– начисление взносов в пенсионный фонд, фонд социального страхования;

– начисление налога на доход физических лиц;

– формирование отчётности для предоставления в государственные органы власти;

– обеспечение общехозяйственной деятельности;

– обеспечение экономической, информационной, физической и пожарной безопасности;

– предотвращение конфликта интересов.

4.4. Целями обработки персональных данных уволенных работников Учреждения являются:

– ведение кадрового делопроизводства;

– формирование отчётности для предоставления в государственные органы.

4.5. Целями обработки персональных данных членов семей работников Учреждения являются:

– учёт налоговых льгот при начислении заработной платы;

– исполнение обязанностей работодателя при возникновении несчастного случая.

5. Категории субъектов персональных данных

5.1. К субъектам персональных данных относятся:

– физические лица, состоящие (состоявшие) в трудовых отношениях с учреждением (далее – работники);

– кандидаты на замещение вакантных должностей в МКУ «ЕДДС Дзержинский»;

– ближайшие родственники работников учреждения;

– граждане Российской Федерации, проживающие или находящиеся на территории муниципального образования «Городской округ Дзержинский», обратившиеся к оператору для передачи информации (сообщения) и вызова экстренных оперативных служб по единому номеру «112», передачи информации для обеспечения общественной и промышленной безопасности, обеспечения функционирования систем жизнедеятельности города, для получения справочной или консультативной информации в области обеспечения общественной и промышленной безопасности на территории городского округа Дзержинский, соседних образованиях, других субъектах;

– граждане иностранных государств для передачи информации (сообщения) и вызова экстренных оперативных служб по единому номеру «112»;

– физические и юридические лица или их уполномоченные представители, обратившиеся в Учреждение для передачи информации или с запросом на предоставление законной информации по вопросам справочной или консультативной помощи.

5.2. Перечень персональных данных, обрабатываемых в Учреждении, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами МКУ «ЕДДС Дзержинский» с учётом целей обработки персональных данных.

5.3. Обработка персональных данных работников учреждения, граждан, претендующих на замещение вакантных должностей в МКУ «ЕДДС Дзержинский» осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, обеспечения кадровой работы, содействия работникам Учреждения в исполнении специальных должностных обязанностей, формирования кадрового резерва, содействия в обучении и должностном росте, обеспечения личной безопасности работников и членов их семей а также в целях обеспечения сохранности принадлежащего им имущества и имущества МКУ «ЕДДС Дзержинский», обеспечения работникам учреждения установленных законодательством Российской Федерации условий труда, гарантий и компенсаций, учёта результатов исполнения ими должностных обязанностей, а также в целях противодействия коррупции.

6. Порядок обработки персональных данных

6.1. Получение персональных данных сотрудников учреждения и персональных данных субъектов персональных данных

6.1.1. Обработка персональных данных субъектов персональных данных, указанных в п. 5.1 Политики, осуществляется следующими структурными подразделениями ЕДДС:

- управление;
- центр управления.

6.1.2. Обработка персональных данных субъектов персональных данных включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

6.1.3. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных осуществляется путём получения персональных данных непосредственно от субъектов персональных данных либо их законных представителей.

6.1.4. Уполномоченные работники Учреждения получают сведения о персональных данных работников МКУ «ЕДДС Дзержинский» при оформлении трудовых отношений и замещения вакантных, из следующих документов:

– паспорт или иной документ, удостоверяющий личность;
– трудовая книжка или документ, подтверждающий трудовой стаж;
– страховое свидетельство государственного пенсионного страхования;
– документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
– документ об образовании, о квалификации или наличии специальных знаний;
– свидетельство о присвоении ИНН;
– анкета, заполняемая при приёме на работу;
– справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования;
– медицинское заключение о прохождении медицинских осмотров и отсутствии медицинских противопоказаний для выполнения трудовых функций в Учреждении;
– свидетельства о государственной регистрации актов гражданского состояния;
– наградные листы;
– иные документы и сведения, предоставляемые субъектом персональных данных при приёме на работу), а также в процессе трудовой деятельности.

6.1.5. При оформлении работника в ЕДДС уполномоченным работником заполняется унифицированная форма Т-2 «Личная карточка», в которой отражаются следующие анкетные и биографические данные работника:

– общие сведения (Ф.И.О.) работника, дата рождения, место рождения, гражданство, знание иностранного языка, образование, учёная степень, профессия, стаж работы, состояние в браке, состав семьи, паспортные данные, адрес места жительства, номер телефона);
– сведения о воинском учёте;
– данные о приёме на работу;

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;
– сведения о присвоении квалификационного разряда, классного чина, дипломатического ранга, воинского звания;
– сведения об аттестации;
– сведения о повышении квалификации;
– сведения о профессиональной переподготовке;
– сведения о наградах (поощрениях), почётных званиях;
– сведения об отпусках;
– сведения о социальных льготах;
– основания прекращения трудового договора (увольнения).

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

6.1.7. Работник, ответственный за документационное обеспечение, принимает от субъекта персональных данных документы, проверяет их полноту и правильность указываемых сведений.

6.1.8. При сборе персональных данных работники учреждения, осуществляющие сбор (получение) персональных данных непосредственно от субъектов персональных данных, обязаны разъяснить указанным субъектам персональных данных юридические последствия отказа предоставить их персональные данные.

6.1.9. В случае возникновения необходимости получения персональных данных субъекта персональных данных у третьей стороны следует известить об этом субъекта персональных данных заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных.

6.2. Обработка персональных данных

6.2.1. Обработка персональных данных субъектов персональных данных, указанных в п. 5.1 настоящей Политики, может осуществляться без согласия указанных лиц в рамках целей, в соответствии с пунктами 2, 4, 11 части 1 статьи 6 и частью 2 статьи 11 Федерального закона «О персональных данных», Федерального закона «О противодействии коррупции», Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Административным кодексом Российской Федерации.

6.2.2. Обработка специальных категорий персональных данных субъектов персональных данных может осуществляться без согласия указанных лиц в рамках целей, определённых пунктом 5.3 настоящего Порядка, в соответствии с подпунктом 2.3 пункта 2 части 2 статьи 10 Федерального закона «О персональных данных» и положениями Трудового кодекса Российской Федерации, за исключением случаев получения персональных данных работника Учреждения у третьей стороны.

6.2.3. Обработка персональных данных субъектов персональных данных осуществляется при условии получения согласия указанных лиц в следующих случаях:

– при передаче (распространении, предоставлении) персональных данных третьим лицам в случаях, не предусмотренных действующим законодательством Российской Федерации;

– при принятии решений, порождающих юридические последствия в отношении указанных лиц или иным образом затрагивающих их права и законные интересы, на основании исключительно автоматизированной обработки их персональных данных.

6.2.4. В случаях, предусмотренных пунктом 6.2.3 настоящего Порядка, согласие субъекта персональных данных оформляется в письменной форме, если иное не установлено Федеральным законом «О персональных данных».

6.2.5. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных осуществляется путём:

– получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в Учреждение);

– копирования оригиналов документов;

– внесения сведений в учётные формы (на бумажных и электронных носителях);

– формирования персональных данных о физических и юридических лицах (объектах персональных данных) в ходе деятельности Учреждения.

6.2.6. Документы, содержащие персональные данные работников Учреждения, составляют его личное дело. Личное дело ведётся на протяжении всей его служебной деятельности. Изменения, вносимые в личное дело, подтверждаются соответствующими документами. В личное дело работника вносятся его персональные данные и иные сведения, связанные с поступлением на работу, её прохождением и увольнением с работы и необходимые для обеспечения деятельности Учреждения.

6.2.7. Персональные данные, внесённые в личные дела работников, иные сведения, содержащиеся в личных делах, относятся к сведениям конфиденциального характера (за исключением сведений, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации). К личному делу приобщаются документы, предусмотренные федеральными законами и иными нормативными правовыми актами Российской Федерации.

6.2.8. Для хранения персональных данных на бумажных и электронных носителях используются специально оборудованные шкафы или сейфы, которые запираются на ключ. Ключ от шкафов и сейфов, в которых хранятся персональные данные, находится у уполномоченного лица.

6.2.9. Персональные данные субъектов персональных данных могут проходить дальнейшую обработку и передаваться на хранение в электронном виде: в локальной компьютерной сети и программно-аппаратных комплексах.

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

6.2.11. В работников Учреждения, осуществляющих обработку персональных данных,

входит:

– обеспечение сохранности документов, содержащих персональные данные;

– обеспечение конфиденциальности персональных данных, в соответствии с федеральными законами, иными нормативными правовыми актами Российской Федерации, а также в соответствии с настоящим Порядком.

6.2.12. Сроки обработки и хранения персональных данных субъектов персональных данных определяются в соответствии с законодательством Российской Федерации и Приказом Минкультуры России от 25.08.2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения».

6.2.13. Персональные данные работников Учреждения, в том числе родственников работника, используются в течение трудовой деятельности в соответствии с трудовым договором, а также на протяжении установленного законодательством срока хранения личного дела в архиве (75 лет).

6.2.14. Обработка персональных данных граждан и юридических лиц, обратившихся к оператору, прекращается в соответствии с нормативно-правовыми актами и регламентами, определяющими функции оператора.

6.3. Доступ к персональным данным

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

6.3.2. Процедура оформления доступа работника к обработке персональных данных (ПДн) включает в себя:

– ознакомление работника под личную подпись с внутренними документами, содержащими требования по обработке и обеспечению безопасности ПДн в части, касающейся их должностных обязанностей.

– истребование с работника письменного обязательства о соблюдении режима конфиденциальности персональных данных, в соответствии с утверждённой формой. Данное обязательство хранится в личном деле работника.

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

6.3.4. Внешний доступ со стороны третьих лиц к персональным данным субъектов персональных данных осуществляется с их письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъектов, и иных случаев, установленных законодательством.

6.4. Передача персональных данных

6.4.1. Передача (распространение, предоставление) и использование персональных данных субъектов персональных данных осуществляется лишь в случаях и в порядке, предусмотренных федеральными законами.

6.4.2. При передаче персональных данных запрещается:

– сообщать персональные данные субъекта персональных данных третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, предусмотренных федеральными законами;

– сообщать персональные данные субъекта персональных данных в коммерческих целях без

его письменного согласия.

6.4.3. При передаче персональных данных уполномоченные работники предупреждают лиц, получающих персональные данные субъекта персональных данных, 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 субъекта персональных данных, обязаны соблюдать режим конфиденциальности.

6.4.4. Передача персональных данных субъекта персональных данных представителям субъекта персональных данных осуществляется в порядке, установленном федеральными законами. Передаваемая информация ограничивается только теми персональными данными субъекта персональных данных, которые необходимы для выполнения указанными представителями их функций.

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

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

6.4.7. Передача персональных данных субъекта третьим лицам осуществляется только с письменного согласия субъекта, которое оформляется по установленной форме. Согласие субъекта на передачу его персональных данных третьим лицам не требуется в случаях, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта; когда согласие субъекта на передачу его персональных данных третьим лицам получено от него в письменном виде при заключении договора с Учреждением; когда третьи лица оказывают услуги Учреждения на основании заключённых договоров, а также в случаях, установленных федеральным законом и настоящим Порядком.

6.4.8. Работники, передающие персональные данные субъектов третьим лицам, должны передавать их с обязательным составлением акта приёма-передачи документов (иных материальных носителей), содержащих персональные данные субъектов. Передача документов (иных материальных носителей), содержащих персональные данные субъектов, осуществляется при наличии у лица, уполномоченного на их получение:

– соглашения об информационном взаимодействии с Учреждением;

– соглашения о неразглашении конфиденциальной информации либо наличие в договоре с третьим лицом пунктов о неразглашении конфиденциальной информации, в том числе, предусматривающих защиту персональных данных субъекта;

– письма-запроса от третьего лица, которое должно включать в себя указание на основания получения доступа к запрашиваемой информации, содержащей персональные данные субъекта, её перечень, цель использования, Ф.И.О. и должность лица, которому поручается получить данную информацию.

6.4.9. Факт передачи персональных данных субъекта регистрируются в «Журнале учёта передачи персональных данных». В журнале фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, перечень передаваемой информация. Ответственность за соблюдение вышеуказанного порядка предоставления персональных данных субъекта несут работники Учреждения и их непосредственные руководители.

6.4.10. Представителю субъекта (в том числе адвокату) персональные данные передаются в порядке, установленном действующим законодательством и настоящим Порядком. Информация передаётся при наличии одного из документов:

– нотариально удостоверенной доверенности представителя субъекта;

– письменного заявления субъекта, написанного в присутствии уполномоченного работника Учреждения.

Доверенности и заявления приобщаются к совокупности документов субъекта персональных

данных.

6.4.11. Документы, содержащие персональные данные субъекта, могут быть отправлены через организацию федеральной почтовой связи. При этом должна быть обеспечена их конфиденциальность. Документы, содержащие персональные данные, вкладываются в конверт, к нему прилагается сопроводительное письмо. На конверте делается надпись о том, что содержимое конверта является конфиденциальной информацией, и за незаконное её разглашение законодательством предусмотрена ответственность. Далее конверт с сопроводительным письмом вкладывается в другой конверт, на который наносятся только реквизиты, предусмотренные почтовыми правилами для заказных почтовых отправлений.

6.4.12. Трансграничная передача персональных данных запрещена.

6.5. Уточнение, изменение, блокирование персональных данных

6.5.1. 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 внесённых изменениях и предпринятых мерах оператор обязан уведомить субъекта персональных данных и третьих лиц, которым персональные данные этого субъекта были переданы.

6.5.2. 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.

6.5.3. 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.

6.5.4. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путём обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путём фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путём изготовления нового материального носителя с уточненными персональными данными.

6.6. Уничтожение персональных данных

6.6.1. 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.

6.6.2. В случае выявления неправомерной обработки персональных данных Учреждение в срок, не превышающий трёх 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.

6.6.3. 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.

6.6.4. 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.

6.6.5. Перед уничтожением ПДн необходимо:

– убедиться в правовых основаниях уничтожения ПДн;

– убедиться в том, что уничтожаются именно те ПДн, которые предназначены для уничтожения;

– уничтожить ПДн подходящим способом, указанным в соответствующем требовании или распорядительном документе;

– проверить необходимость уведомления об уничтожении ПДн субъекта ПДн, или его представителя, или третьих лиц в предусмотренном случае.

6.6.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7. Права субъектов персональных данных

7.1. В целях обеспечения защиты персональных данных субъекты персональных данных имеют право:

– получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

– осуществлять по запросу свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом;

– требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона. Субъект персональных данных при отказе Учреждения исключить или исправить персональные данные имеет право заявить в письменной форме Учреждению о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект персональных данных имеет право дополнить заявлением, выражающим его собственную точку зрения;

– требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта персональных данных, обо всех произведенных в них изменениях или исключениях из них;

– обжаловать в суд любые неправомерные действия или бездействие Учреждения при обработке и защите персональных данных субъекта персональных данных.

7.2. 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.

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

7.4. Порядок взаимодействия с субъектами персональных данных, обрабатываемых в информационных системах Учреждения:

Порядок (процедура) взаимодействия с субъектами ПДн включает в себя приём, обработку и подготовку ответа на заявление или обращение субъекта ПДн.

Взаимодействие с субъектом ПДн осуществляется на основании обращения или запроса субъекта персональных данных (его законного представителя).

Факт получения обращения или запроса от субъекта персональных данных и результаты их рассмотрения (проделанной работы по обращению или запросу) фиксируется в соответствии с регламентом обращений субъектов персональных данных.

Виды взаимодействия с субъектом ПДн:

– взаимодействие, связанное с выполнением служебных полномочий Учреждения в соответствии с регламентами;

– взаимодействие, связанное с реализацией прав субъектов ПДн в соответствии с Федеральным законом «О персональных данных» (далее – взаимодействие по реализации прав субъектов ПДн).

Субъект персональных данных или его законный представитель имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных;

– правовые основания и цели обработки персональных данных;

– цели и применяемые оператором 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 субъекту персональных данных, источник их получения, если иной порядок предоставления 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»;

– информацию об осуществлённой или о предполагаемой трансграничной передаче 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.

Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их обезличивания или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами (ч. 8 ст. 14 Федерального закона «О персональных данных»).

Если в результате рассмотрения обращения (запроса) субъекта персональных данных или его представителя выявятся случаи неправомерной обработки персональных данных или обработки персональных данных, являющихся неполными, неточными, устаревшими, незаконно полученными, избыточными по отношению к целям обработки персональных данных, сотрудники Учреждения обязаны устранить допущенные нарушения в срок, не превышающий трёх рабочих дней с даты выявления.

Сотрудники, уполномоченные осуществлять взаимодействие с субъектами ПДн, несут

административную, дисциплинарную и иную, предусмотренную законодательством Российской Федерации, ответственность за нарушение прав субъектов ПДн, произошедшее по их вине.

8. Меры, направленные на обеспечение безопасности персональных данных

8.1. Общие меры

8.1.1. 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 защиты 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;

– издаёт 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.

8.1.2. Работники Учреждения, ответственные за хранение персональных данных, а также работники Учреждения, владеющие персональными данными в силу своих должностных обязанностей, подписывают обязательство о неразглашении информации.

8.1.3. Помещения, в которых хранятся персональные данные, оборудуются сейфами или закрывающими на ключ шкафами, надёжными замками. В рабочее время при отсутствии работников помещения запираются на ключ. Проведение уборки помещений, в которых хранятся персональные данные, производится в соответствии с регламентом внутри объектового режима.

8.1.4. Лицо, ответственное за организацию обработки персональных данных в Учреждении, осуществляет 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.

8.1.5. 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.

8.2. Меры, направленные на обеспечение безопасности персональных данных при их обработке в информационных системах

8.2.1. Обработка персональных данных субъектов персональных данных, указанных в п. 5.1 настоящего Порядка, осуществляется в информационных системах персональных данных (ИСПДн)

на автоматизированных рабочих местах (АРМ) Учреждения, как с помощью программно-аппаратных комплексов (ПАК), так и без них.

8.2.2. Классификация информационных систем, указанных в пункте 8.2.1 настоящего Порядка, осуществляется в порядке, установленном законодательством Российской Федерации.

8.2.3. Работникам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах Учреждения, предоставляется уникальный логин и пароль для доступа к информационным системам. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными регламентами.

8.2.4. Для обеспечения безопасности ПДн при их обработке в ИСПДн осуществляется защита информации, обрабатываемой техническими средствами, под которыми понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных, программные средства, средства защиты информации.

8.2.5. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного доступа к персональным данным, результатом которого может стать уничтожение, блокирование, изменение, копирование, распространение персональных данных, а также иных несанкционированных действий, а также принятия следующих мер по обеспечению безопасности:

– определение угроз безопасности персональных данных при их обработке в информационной системе;

– применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни (классы) защищённости персональных данных;

– применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

– оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы;

– учёт машинных носителей персональных данных;

– обнаружение фактов несанкционированного доступа к персональным данным и принятие мер реагирования;

– восстановление персональных данных, модифицированных или удалённых, уничтоженных вследствие несанкционированного доступа к ним;

– установление правил доступа к персональным данным, обрабатываемым в информационных системах, а также обеспечением регистрации и учёта всех действий, совершаемых с персональными данными в информационных системах;

– контроль принимаемых мер по обеспечению безопасности персональных данных и уровня (класса) защищённости информационной системы.

8.2.6. Организуется режим защиты помещений, в которых осуществляется обработка персональных данных, размещение технических средств ИСПДн, машинных носителей информации, исключающий возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

8.2.7. Все магнитные, оптические и другие съёмные машинные носители ПДн подлежат обязательному учёту. На носители информации наносится маркировка, позволяющая идентифицировать и организовать их учёт. Машинные носители информации, в том числе с резервными копиями ПДн, регистрируются в журнале учёта машинных носителей ПДн, в котором отражается:

– тип и ёмкость носителя;

– учётный номер носителя;

– место установки (использования) носителя;

– дата установки носителя;

– ответственное должностное лицо;

– сведения о списании носителя и уничтожении информации.

8.2.8. Пользователям запрещается использовать съёмные носители информации за исключением случаев, когда использование съёмных носителей необходимо в рамках должностных обязанностей.

8.2.9. Структурное подразделение (ответственное лицо) Учреждения, ответственное за защиту информации в Учреждения, организует и контролирует ведение учёта материальных носителей персональных данных.

8.2.10. Структурное подразделение (ответственное лицо) Учреждения, ответственное за обеспечение безопасности персональных данных при их обработке в информационных системах (администратор безопасности ПДн), обеспечивает:

– своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Учреждения;

– недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

– возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– постоянный контроль за обеспечением уровня защищённости персональных данных;

– знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– учёт применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– принятие всех необходимые меры по восстановлению персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним;

– при обнаружении нарушений порядка предоставления персональных данных – незамедлительное приостановление предоставления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин;

– разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

8.2.11. Обмен персональными данными при их обработке в информационных системах Учреждения осуществляется по каналам связи, защита которых обеспечивается путём реализации соответствующих организационных мер и путём применения программных и технических средств.

8.3. Меры, направленные на обеспечение безопасности персональных данных при их обработке без использования средств автоматизации

8.3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, осуществляется таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

8.3.2. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных.

8.3.3. Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

8.3.4. Работники Учреждения, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими

персональных данных, обработка которых осуществляется в Учреждения без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных законодательством и локальными нормативными актами Учреждения.

8.3.5. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, принимаются меры по обеспечению раздельной обработки персональных данных, в частности:

– при необходимости использования или распространения определённых персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

– при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

8.3.6. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее – типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по её заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, полное наименование и адрес Учреждения, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки ПДн;

– типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на обработку ПДн, осуществляемую без использования средств автоматизации, – при необходимости получения письменного согласия на обработку ПДн;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн;

– типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

8.3.7. При ведении журналов (реестров, книг), содержащих ПДн, необходимых для однократного пропуска субъекта ПДн на территорию Учреждения, или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена локальным актом Учреждения, содержащим сведения о цели обработки ПДн, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов ПДн, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки ПДн, а также сведения о порядке пропуска субъекта ПДн на территорию, на которой находится Учреждение, без подтверждения подлинности ПДн, сообщённых субъектом ПДн;

– копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

– ПДн каждого субъекта ПДн могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта ПДн на территорию Учреждения.

8.3.8. Уничтожение или обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих ПДн с

сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

8.3.9. Уточнение ПДн при осуществлении их обработки без использования средств автоматизации производится путём обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, – путём фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путём изготовления нового материального носителя с уточнёнными ПДн.

9. Правила работы с обезличенными данными (в случае обезличивания персональных данных)

9.1. Обезличивание персональных данных в Учреждения проводится с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижении 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 путём замены результатами статистической обработки, обобщения, преобразования или удаления части сведений;
- декомпозиция (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств);
- перемешивание (перестановка отдельных записей, а также групп записей в массиве персональных данных).

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 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 съёмными 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. Порядок взаимодействия с уполномоченным органом по защите прав субъектов персональных данных

10.1. В целях уведомления уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) лицо, ответственное за организацию обработки персональных данных в Учреждения, направляет уведомление о внесение изменений в сведения в реестре операторов, осуществляющих обработку персональных данных, в следующих случаях:

– при вводе в эксплуатацию новых информационных систем персональных данных в Учреждения;

– при внесении изменений в существующие информационные системы персональных данных Учреждения.

10.2. Уведомление направляется в виде документа на бумажном носителе или в форме электронного документа и подписывается руководителем Учреждения.

10.3. Уведомление должно содержать следующие сведения:

– наименование, адрес Учреждения;

– цель обработки персональных данных;

– категории персональных данных;

– категории субъектов, персональные данные которых обрабатываются;

– правовое основание обработки персональных данных;

– перечень действий с персональными данными, общее описание используемых Учреждением способов обработки персональных данных;

– описание принятых мер защиты персональных данных, в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;

– фамилию, имя, отчество работника Учреждения, ответственного за организацию обработки персональных данных, и номера контактных телефонов, почтовые адреса и адреса электронной почты;

– дату начала обработки персональных данных;

– срок или условие прекращения обработки персональных данных;

– сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

– сведения о месте нахождения базы данных информации, содержащей персональные данные граждан Российской Федерации;

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

10.4. Лицо, ответственное за организацию обработки персональных данных в Учреждения, осуществляет контроль соответствия сведений, внесённых уполномоченным органом по защите прав субъектов персональных данных в реестр операторов. Сведения, содержащиеся в реестре операторов, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, являются общедоступными.

10.5. В случае изменения сведений, указанных в п. 10.3 Порядка, а также в случае прекращения обработки персональных данных лицо, ответственное за организацию обработки персональных данных в Учреждения, обязано уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

10.6. При получении запроса от уполномоченного органа по защите прав субъектов персональных данных лицо, ответственное за организацию обработки персональных данных в Учреждения, осуществляет подготовку и направление ответа в течение тридцати дней с даты получения такого запроса.

11. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

11.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными актами в Учреждения организуется проведение периодических проверок условий обработки персональных данных с последующей регистрацией в «Журнале учёта проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных».

11.2. Проверки осуществляются ответственным за организацию обработки персональных данных в Учреждения либо комиссией, инициируемой руководителем Учреждения.

11.3. В проведении проверки не может участвовать работник Учреждения, прямо или косвенно заинтересованный в её результатах.

11.4. Проверки соответствия обработки персональных данных установленным требованиям в Учреждения проводятся на основании утверждённого ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в Учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трёх рабочих дней с момента поступления соответствующего заявления.

11.5. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

– порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных;

– порядок и условия применения средств защиты информации;

– эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

– состояние учёта машинных носителей персональных данных;

– соблюдение правил доступа к персональным данным;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

– мероприятия по восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– осуществление мероприятий по обеспечению целостности персональных данных.

11.6. Ответственный за организацию обработки персональных данных в Учреждении (комиссия) имеет право:

– запрашивать у работников Учреждения информацию, необходимую для реализации полномочий;

– требовать от уполномоченных на обработку персональных данных работников уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путём персональных данных;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

– вносить руководителю Учреждения предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

– вносить руководителю Учреждения предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

11.7. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в Учреждении (комиссии) в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

11.8. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведённой проверки и мерах, необходимых для устранения выявленных нарушений, руководителю Учреждения докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

11.9. Руководитель Учреждения обязан контролировать своевременность и правильность проведения проверки.

12. Оценка вреда, который может быть причинён субъектам персональных данных в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

12.1. Оценкой вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», является определение юридических последствий в отношении субъекта ПДн.

12.2. К юридическим последствиям относятся случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или иным образом затрагивающее его права, свободы и законные интересы.

12.3. При обработке ПДн должны определяться и документально оформляться все возможные юридические или иным образом затрагивающие права и законные интересы последствия в отношении субъекта ПДн, которые могут возникнуть в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

12.4. Определение таких юридических последствий необходимо для недопущения нарушения и обеспечения защиты прав и свобод человека, и гражданина при обработке его ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

12.5. Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» оформляется документально.

12.6. Во время осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн производится оценка соотношения вреда, который может быть причинён субъектам ПДн и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

12.7. При оценке соотношения вреда, который может быть причинён субъектам ПДн, для каждой ИСПДн производится экспертное сравнение заявленной Учреждением в своих локальных актах оценки вреда, который может быть причинён субъектам ПДн, и применяемых мер, направленных на выполнение обязанностей, предусмотренных Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», и изложенных в настоящем Порядке.

12.8. По итогам сравнений принимается решение о достаточности применяемых мер, направленных на обеспечение выполнения обязанностей, предусмотренных действующим законодательством в области ПДн, и возможности или необходимости принятия дополнительных мер или изменения установленного порядка организации и проведения работ по обеспечению безопасности ПДн при их обработке.

13. Порядок проведения служебных проверок по фактам нарушения требований по обеспечению безопасности персональных данных

13.1. Классификация нарушений требований по обеспечению безопасности персональных данных.

Нарушения требований по обеспечению безопасности ПДн и их последствия классифицируются по значимости на:

- нарушения I категории;
- нарушения II категории;
- нарушения III категории.

Служебная проверка назначается по нарушениям I и II категорий.

13.2. Перечень нарушений требований по обеспечению безопасности персональных данных.

Нарушения I категории, к которым относятся нарушения, повлекшие за собой разглашение (утечку), уничтожение (искажение) ПДн и/или утрату машинных носителей ПДн, выведение из строя технических и программных средств, входящих в состав ИСПДн, а именно:

- успешный подбор административного пароля;
- несанкционированная реконфигурация параметров ИСПДн;
- утрата или кража резервной копии базы, содержащей ПДн;
- необоснованная передача информационных массивов ИСПДн;
- организация утечки сведений по техническим каналам;
- умышленное нарушение работоспособности ИСПДн;
- НСД к ПДн;
- несанкционированное внесение изменений в ИСПДн;
- умышленное заражение персональных электронных вычислительных машин (далее – ПЭВМ) и серверов, входящих в состав ИСПДн, вирусами;
- проведение работ с ИСПДн, повлекшее за собой необратимую потерю данных;
- другие действия, попадающие под действия статей, приведённых в следующей таблице:

Номер статьи	Название статьи
Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и о защите информации»	
ст. 17	Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации
Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»	
ст. 24	Ответственность за нарушение требований настоящего Федерального закона
Кодекс Российской Федерации об административных правонарушениях	
ст. 13.11	Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (ПДн)
ст. 13.11.1	Распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера
ст. 13.12	Нарушение правил защиты информации
ст. 13.14	Разглашение информации с ограниченным доступом
Уголовный кодекс Российской Федерации	
ст. 137	Нарушение неприкосновенности частной жизни
ст.140	Отказ в предоставлении гражданину информации
ст. 272	Неправомерный доступ к компьютерной информации
ст. 273	Создание, использование и распространение вредоносных компьютерных программ

Номер статьи	Название статьи
ст. 274	Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
Трудовой кодекс Российской Федерации	
ст. 90	Ответственность за нарушение норм, регулирующих обработку и защиту ПДн работника

Нарушения II категории, к которым относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке), уничтожению (искажению) ПДн, утрате машинных носителей ПДн, выведению из строя технических и программных средств, входящих в состав ИСПДн, а именно:

– ошибка при входе в ИСПДн (набор не назначенного пароля, более 3 (трёх) раз подряд, периодически);

– оставление ПЭВМ включённой (незаблокированной) во время отсутствия на рабочем месте;

– перезагрузка ПЭВМ при сбоях в работе, в т.ч. аварийная (неоднократная) перезагрузка путём нажатия кнопки RESET;

– утрата учтённого машинного носителя ПДн;

– многократная неудачная попытка входа под чужим именем, паролем;

– удачная попытка входа под чужим именем, паролем;

– несанкционированная очистка журналов аудита;

– несанкционированное копирование ПДн на внешние носители информации;

– несанкционированная установка (удаление) программного обеспечения (далее – ПО) в ИСПДн;

– несанкционированное изменение конфигурации ПО ИСПДн;

– попытка получения прав администратора на ПЭВМ (увеличения полномочий собственных прав, получение прав на отладку программ) удачная и неудачная;

– попытка получения прав администратора в домене или на удалённой машине, удачная и неудачная;

– неумышленное заражение ПЭВМ компьютерными вирусами;

– несанкционированное использование сканирующего ПО;

– несанкционированное использование анализаторов протоколов (снифферов);

– несанкционированный просмотр, вывод на печать и т.п. ПДн.

Нарушения III категории, к каковым относятся нарушения, не несущие признаков нарушений I и II категорий, а именно:

– ошибка при входе в ИСПДн (набор неправильного пароля, сетевого имени более 3 (трёх) раз подряд, не периодическая);

– периодическая попытка неудачного доступа к ПДн ИСПДн;

– перевод времени на ПЭВМ;

– однократная перезагрузка ПЭВМ при сбоях в работе ПЭВМ, в т.ч. аварийная перезагрузка, путём нажатия кнопки RESET;

– нецелевое использование корпоративных ресурсов (печать, доступ в сеть Internet, электронная почта и т.п.).

13.3. Назначение и проведение служебных проверок.

Служебная проверка назначается по нарушениям I и II категорий.

Служебная проверка может быть инициирована на основании устного заявления, докладной или служебной записки любого работника по выявленному отдельному факту нарушения, либо по факту группы нарушений.

Служебная проверка проводится комиссией, состав которой утверждает руководитель Учреждения. Члены комиссии имеют право:

– требовать документального подтверждения факта нарушения;

– устанавливать причины допущенных нарушений любым из способов, не противоречащим

законодательству Российской Федерации;

– брать письменные объяснения по поводу выявленных нарушений у любого работника.

13.4. Оформление результатов работы комиссии.

Результаты работы комиссии должны быть оформлены в виде аналитического экспертного заключения, в котором отражается:

– состав комиссии;

– период времени, в течение которого проводилась служебная проверка;

– основание для проведения служебной проверки;

– документальное подтверждение фактов нарушений, выявленных в ходе служебной проверки и имеющих значение в определении наличия нарушений, а также иных фактов, которые могут привести к нарушению конфиденциальности ПДн или к снижению уровня защищенности ПДн;

– установленные причины выявленных нарушений;

– вывод о значимости нарушений, их причинах и виновных, допустивших данные нарушения;

– рекомендации по совершенствованию обеспечения безопасности ПДн, исключающие в дальнейшем подобные нарушения.

14. Порядок приостановления обработки персональных данных

При обнаружении нарушений I категории обработка ПДн незамедлительно приостанавливается до выявления причин нарушений и устранения этих причин.

Принятие решения о приостановлении обработки ПДн принимается руководителем Учреждения.

По факту нарушения требований по обеспечению безопасности, повлекшего приостановление обработки ПДн, проводится служебная проверка.

15. Порядок обращения со средствами защиты информации

15.1. Учёт средств защиты информации.

Под средствами защиты информации (далее – СЗИ) в настоящем разделе понимается СЗИ, не являющееся средствами криптографической защиты (далее – СКЗИ).

Инсталлирующие СЗИ носители, установленные СЗИ, эксплуатационная и техническая документация к СЗИ подлежат поэкземплярному учёту в «Журнале учета средств защиты информации, эксплуатационной и технической документации к ним» (Формуляре).

15.2. Распространение средств защиты информации.

СЗИ доставляются фельдъегерской (в том числе ведомственной) связью или со специально выделенными работниками при соблюдении мер, исключающих бесконтрольный доступ к СЗИ во время доставки.

При пересылке СЗИ помещаются в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия. Эксплуатационная и техническая документация к СЗИ пересылается заказными, ценными почтовыми отправлениями или доставляется специально выделенными работниками.

При пересылке СЗИ, эксплуатационной и технической документации к ним подготавливается сопроводительное письмо, в котором указывается: что посылается и в каком количестве, учётные номера изделий или документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывается в одну из упаковок.

Отправитель контролирует доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель направляет ему запрос и принимает меры к уточнению местонахождения отправлений.

15.3. Получение средств защиты информации.

Полученные упаковки вскрываются только лицом, для которого они предназначены.

Если содержимое полученной упаковки не соответствует указанному в сопроводительном

письме или сама упаковка и печать – их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к её содержимому, то получателем составляется акт, который высылается отправителю. Полученные с такими отправлениями СЗИ до получения указаний от отправителя применять не разрешается.

При обнаружении бракованных СЗИ один экземпляр бракованного изделия возвращается отправителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранятся до поступления дополнительных указаний от отправителя.

Получение СЗИ, эксплуатационной и технической документации к ним подтверждается отправителю в соответствии с порядком, указанным в сопроводительном письме.

15.4. Уничтожение средств защиты информации.

СЗИ уничтожаются (утилизируются) по решению руководителя Учреждения.

Намеченные к уничтожению (утилизации) СЗИ изымаются из аппаратных средств, с которыми они функционировали. При этом СЗИ считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СЗИ процедура удаления программного обеспечения СЗИ и они полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения используются после уничтожения СЗИ без ограничений.

Уничтожение большого объёма инсталлирующих СЗИ носителей оформляется актом. Уничтожение по акту производится комиссией в составе не менее трёх человек из числа лиц, допущенных к работе с СЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых инсталлирующих СЗИ носителей. Исправления в тексте акта оговариваются и заверяются подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в журнале учёта средств защиты информации, эксплуатационной и технической документации к ним.

Эксплуатационная и техническая документация к СЗИ уничтожается путём сжигания или с помощью любых бумагорезательных машин. Факт уничтожения эксплуатационной и технической документации к СЗИ оформляется в журнале учёта средств защиты информации, эксплуатационной и технической документации к ним.

15.5. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены средства защиты информации

Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены СЗИ, должны обеспечивать сохранность ПДн, СЗИ, исключать возможность неконтролируемого проникновения или пребывания в помещениях, где установлены СЗИ, посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

При оборудовании помещений, где установлены СЗИ, должны выполняться требования к размещению и монтажу СЗИ, а также другого оборудования, функционирующего с СЗИ.

Инсталлирующие СЗИ носители, эксплуатационная и техническая документация к СЗИ должны храниться в металлических хранилищах (ящиках, шкафах, помещениях) в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Помещения, где установлены СЗИ, должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время.

Для предотвращения просмотра извне помещений, где установлены СЗИ, их окна должны быть оборудованы шторами или жалюзи.

16. Ответственность за нарушение требований, регулирующих получение, обработку и хранение персональных данных

16.1. Работники Учреждения, уполномоченные на обработку персональных данных, могут привлекаться в соответствии с законодательством Российской Федерации к дисциплинарной и иной ответственности за разглашение конфиденциальных сведений, содержащихся в указанных личных

делах, а также за иные нарушения порядка ведения личных дел, установленного законодательством Российской Федерации.

16.2. Лица, виновные в нарушении норм, регулирующих обработку персональных данных, несут административную ответственность по статьям 13.11, 13.14 Кодекса об административных правонарушениях Российской Федерации.

16.3. Предоставление персональных данных посторонним лицам, в том числе работникам Учреждения, не имеющим права их обрабатывать, распространение персональных данных, утрата материальных носителей информации, содержащих персональные данные субъекта, а также иные нарушения обязанностей по обработке персональных данных, установленных настоящим Порядком, локальными актами Учреждения, влечёт наложение на работника, имеющего доступ к персональным данным, дисциплинарного взыскания: замечания, выговора или увольнения.

16.4. Лица, имеющие доступ к персональным данным субъектов, виновные в незаконном сборе или передаче персональных данных, а также осуществившие неправомерный доступ к охраняемой законом компьютерной информации, несут уголовную ответственность в соответствии со статьями 137, 272 Уголовного кодекса Российской Федерации.