

УТВЕРЖДАЮ

Директор

МАУ «РКЦ Образования»



С.Н. Иванова

« 7 » мая 2022 г.

Приложение № 1
к приказу № 6/1 от 17.05.2022 г.

Политика муниципального автономного учреждения "Расчетно-кассового центра в сфере образования Тацинского района" в отношении обработки персональных данных (далее Политика)

1. Общие положения

1.1. Настоящая Политика муниципального автономного учреждения "Расчетно-кассового центра в сфере образования Тацинского района" (далее – Учреждение) в отношении обработки персональных данных определяет принципы, цели, содержание и порядок обработки персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в Учреждении.

1.2. Целью Политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Политика является общедоступным документом, декларирующим основы деятельности Учреждения, связанными с обработкой персональных данных.

1.4. Действие Политики не распространяется на отношения, возникающие при обработке персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.5. В настоящей Политике используются следующие основные понятия, термины и определения, установленные в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных»:

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

Субъект персональных данных — физическое лицо, которое прямо или косвенно определено или определяемо с помощью 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;

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

Неавтоматизированная обработка персональных данных – любые действия с персональными данными, при условии, что использование, уточнение, распространение и уничтожение персональных данных осуществляются при непосредственном участии человека, без использования электронно-вычислительных технологий;

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

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

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

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

1.6. Обработка персональных данных в Учреждении выполняется с использованием средств автоматизации или без использования таких средств. Обработка персональных данных без использования средств автоматизации может осуществляться в виде документов на бумажных носителях и в электронном виде: файлы данных на электронных носителях информации.

2. Принципы и цели обработки персональных данных и соответствующие им перечни обрабатываемых персональных данных

2.1. Обработка персональных данных Учреждении основана на следующих принципах:

2.1.1. Соблюдение законности целей и способов обработки персональных данных.

2.1.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных целей.

2.1.3. Соответствие целей обработки персональных данных целям сбора персональных данных, содержанию и объему обрабатываемых персональных данных.

2.1.4. Недопустимость объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

2.1.5. Обеспечение точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных.

2.1.6. Выполнение правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке.

2.1.7. Соблюдение прав субъекта персональных данных на доступ к его персональным данным.

2.1.8. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

2.1.9. Уничтожение обрабатываемых персональных данных по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Целями обработки персональных данных в Учреждении являются:

2.2.1. Исполнение условий трудового договора, осуществление прав и обязанностей сотрудников Учреждения в соответствии с трудовым законодательством.

2.2.2. Выполнение обязательств по договорам (контрактам) и иным соглашениям, заключаемым Учреждением.

2.2.3. Предоставление услуг, в соответствии с Уставом Учреждения не сотрудникам Учреждения.

2.3. Субъектами обработки персональных данных в Учреждении являются:

2.3.1. Граждане, сотрудники Учреждения, состоящие с Учреждением в отношениях, регулируемых трудовым законодательством.

2.3.2. Граждане, не сотрудники Учреждения – физические лица, персональные данные которых обрабатываются в связи с реализацией уставных полномочий Учреждения, в том числе с предоставлением услуг в соответствии с федеральным законодательством.

2.4. Обработка персональных данных осуществляется с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Согласие субъекта персональных данных должно отвечать требованиям, определенным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

2.5. В целях, указанных в пункте 2.2. настоящей Политики, обрабатываются следующие персональные данные субъектов персональных данных – сотрудников Учреждения:

1) фамилия, имя, отчество (при наличии) (в том числе прежние фамилии, имена и (или) отчества (при наличии), в случае их изменения);

2) дата рождения;

3) место рождения;

4) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи (свидетельство о рождении ребенка);

5) адрес места жительства, дата регистрации по месту жительства (месту пребывания);

6) номер телефона или сведения о других способах связи;

7) сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования или документе, подтверждающем регистрацию в системе индивидуального (персонифицированного) учета;

8) идентификационный номер налогоплательщика;

9) сведения о составе семьи: наличие детей школьного возраста, или обучающихся в училищах или ВУЗах, для предоставления налогового вычета;

10) сведения о трудовой деятельности, включая работу по совместительству;

11) сведения об образовании с указанием наименования образовательной организации, года ее окончания, квалификации, специальности и (или) направления подготовки, наименования и реквизитов документа об образовании;

12) фотография (в личное дело);

- 13) сведения о прежнем месте работы;
- 14) сведения, содержащиеся в трудовом договоре, дополнительных соглашениях к трудовому договору;
- 15) сведения о профессиональной переподготовке и (или) повышении квалификации;
- 16) сведения о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
- 17) номер расчетного счета, для перечисления заработной платы и иных выплат;
- 18) номер банковской карты для перечисления социальных выплат, заработной платы и иных выплат;
- 19) иные сведения, которые субъект персональных данных пожелал сообщить о себе и которые отвечают целям обработки персональных данных, указанным в пункте 2.2 настоящей Политики.

2.6. Обработка персональных данных субъектов персональных данных, указанных в подпункте 2.5. настоящей Политики, 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.

2.7. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных – сотрудников Учреждения осуществляется путем:

- 1) получения оригиналов необходимых документов (заявление, трудовая книжка, автобиография, иные документы, предоставляемые в Учреждение) (далее - оригиналы документов);
- 2) копирования оригиналов документов;
- 3) внесения сведений в учетные формы (на бумажных и электронных носителях);
- 4) формирования персональных данных в ходе кадровой работы;
- 5) внесения персональных данных в информационные системы персональных данных, используемые Учреждением.

2.8. В целях, указанных в пункте 2.2. настоящей Политики, обрабатываются следующие персональные данные субъектов персональных данных – не сотрудников Учреждения с целью предоставления услуг, на основании Устава Учреждения, и услуг на основании муниципальных, региональных и федеральных НПА:

- 1) фамилия, имя, отчество (при наличии) (в том числе прежние фамилии, имена и (или) отчества (при наличии), в случае их изменения);
- 2) дата рождения;
- 3) место рождения;
- 4) вид, серия, номер документа, удостоверяющего личность гражданина Российской Федерации, наименование органа, код подразделения органа, выдавшего его, дата выдачи (свидетельство о рождении для ребенка);
- 5) адрес места жительства, дата регистрации по месту жительства (месту пребывания);
- 6) сведения, содержащиеся в страховом свидетельстве обязательного пенсионного страхования или документе, подтверждающем регистрацию в системе индивидуального (персонифицированного) учета;
- 8) идентификационный номер налогоплательщика;
- 9) сведения о составе семьи: наличие детей дошкольного возраста, школьного возраста, или обучающихся в училищах или ВУЗах, как семей имеющих родственные связи, так и семей детей находящихся под опекой или в приемной семье, для проведения расчётов и выплат, полагающихся в соответствии с законодательством;
- 10) номер расчетного счета для перечисления заработной платы (приемная семья) и иных выплат семей детей, находящихся под опекой;

2.9. Обработка персональных данных субъектов персональных данных, указанных в подпункте 2.8. настоящей Политики, 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.

2.10. Сбор, запись, систематизация, накопление и уточнение (обновление, изменение) персональных данных субъектов персональных данных – не сотрудников Учреждения осуществляется путем:

- 1) получения оригиналов необходимых документов (заявление на предоставление услуги, иные документы, предоставляемые в Учреждение) (далее - оригиналы документов);
- 2) получения копий необходимых документов, в виде пакета документов, указанных в пункте 2.8;
- 3) внесения сведений в учетные формы (на бумажных и электронных носителях);
- 4) формирования персональных данных в ходе работы;
- 5) внесения персональных данных в информационные системы персональных данных, используемые Учреждением.

2.11. Гражданин, претендующий на заключение трудового договора с Учреждением, т.е. будущий сотрудник Учреждения (ознакомлен и принимает содержание данной Политики и данного пункта 2.11.), обязан предоставить свои персональные данные в Учреждение, в виду того, что без предоставления своих персональных данных в МАУ «РКЦ Образования», обязательных для заключения трудового договора согласно ст. 57 и 65 Трудового кодекса Российской Федерации, трудовой договор с данным гражданином не может быть заключен. На основании п. 11 ч. 1 ст. 77 Трудового кодекса Российской Федерации трудовой договор прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность продолжения работы.

2.12. Гражданин, претендующий на получение услуг, предоставляемых Учреждением, т.е. физическое лицо не сотрудник Учреждения (ознакомлен и принимает содержание данной Политики и пункта 2.12.), обязан предоставить свои персональные данные в Учреждение, в виду того, что не предоставление своих персональных данных в МАУ «РКЦ Образования», обязательных для получения услуг, предоставляемых Учреждением в соответствии с Уставом Учреждения, для получателя физического лица не сотрудника Учреждения исключает возможность получения предоставляемых Учреждением услуг (подразумевается передача персональных данных третьему лицу, которым является Учреждение).

2.13. Не допускать обработку и приобщение к личному делу субъекта персональных данных сведений, касающихся состояния здоровья, расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, членства в общественных объединениях или его профсоюзной деятельности, если иное не предусмотрено федеральным законом.

3. Условия и порядок обработки персональных данных субъектов персональных данных в информационных системах

3.1. Обработка персональных данных в Учреждении осуществляется в следующих информационных системах:

- 1) 1С – Бухгалтерия государственного учреждения;
- 2) 1С – Зарплата и кадры государственного учреждения;
- 3) Государственная интегрированная информационная система управления общественными финансами «Электронный бюджет»;
- 4) Единая информационная система управления общественными финансами (ЕАС УОФ);
- 5) Программное обеспечение ФНС России для автоматизации процесса подготовки налогоплательщиком форм документов налоговой и бухгалтерской отчетности и справки по форме 2-НДФЛ («Налогоплательщик ЮЛ»);

б) файлы данных, содержащих сведения о персональных данных.

3.2. Сотрудникам Учреждения, имеющим право осуществлять обработку персональных данных в информационных системах, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе, в соответствии с функциями, предусмотренными должностными регламентами.

3.3. Информация в информационные системы вносится в ручном режиме при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.

3.4. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах, достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным.

3.5. Доступ сотрудников Учреждения к персональным данным, находящимся в информационных системах персональных данных, предусматривает обязательное прохождение процедуры идентификации и аутентификации.

3.6. Обмен персональными данными при их обработке в информационных системах персональных данных (при необходимости) осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и применения программных и технических средств в соответствии со статьей 19 Федерального закона «О персональных данных».

3.7. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Учреждения уполномоченными должностными лицами Учреждения принимаются меры по установлению причин нарушений и их устранению с момента обнаружения таких нарушений.

4. Правила работы с обезличенными данными в случае обезличивания персональных данных

4.1. Обезличивание персональных данных в Учреждении осуществляется в статистических или иных целях с соблюдением требований, установленных подпунктом «з» пункта 1 перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211.

4.2. Персональные данные, полученные в результате обезличивания, могут обрабатываться с использованием и без использования средств автоматизации и не подлежат разглашению.

4.3. Персональные данные, полученные в результате обезличивания, подлежат защите в соответствии с законодательством Российской Федерации.

4.4. Персональные данные, полученные в результате обезличивания, не подлежат предоставлению третьим лицам, осуществляющим обработку персональных данных с использованием дополнительной информации, позволяющей прямо или косвенно определить конкретное физическое лицо.

4.5. При обработке персональных данных, полученных в результате обезличивания, без использования средств автоматизации обеспечивается сохранность содержащих их материальных носителей и порядок доступа сотрудников Учреждения в помещения, в которых они хранятся, в целях исключения несанкционированного доступа к обезличенным персональным данным, возможности их несанкционированного уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий.

4.6. При обработке персональных данных, полученных в результате обезличивания, в информационных системах персональных данных обеспечивается соблюдение парольной защиты информационных систем персональных данных, антивирусной политики, правил работы со съемными носителями (в случае их использования), правил резервного

копирования, правил доступа в помещения, где расположены элементы информационных систем персональных данных.

4.7. При хранении персональных данных, полученных в результате обезличивания, обеспечивается раздельное хранение персональных данных, полученных в результате обезличивания, и информации о выбранном методе обезличивания персональных данных и параметрах процедуры обезличивания персональных данных.

5. Сроки обработки и хранения персональных данных. Порядок уничтожения персональных данных

5.1. Сроки хранения персональных данных в Учреждении определяются в соответствии с Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения, утвержденным приказом Федерального архивного агентства от 20 декабря 2019 г. № 236.

5.2. Срок хранения персональных данных, обрабатываемых в информационных системах персональных данных, соответствует сроку хранения персональных данных на бумажных носителях.

5.3. Персональные данные подлежат уничтожению в следующих случаях:

При достижении цели обработки персональных данных или в случае утраты необходимости в достижении цели обработки персональных данных, если иное не предусмотрено Федеральным законом «О персональных данных»;

При изменении, признании утратившими силу нормативных правовых актов, устанавливающих правовые основания обработки персональных данных;

При выявлении факта неправомерной обработки персональных данных;

При отзыве субъектом персональных данных согласия, если иное не предусмотрено Федеральным законом «О персональных данных».

5.4. В Учреждении, лицами, ответственным за документооборот и архивирование, осуществляется систематический контроль и выявление документов, содержащих персональные данные с истекшими сроками хранения.

5.5. Вопрос об уничтожении документов, содержащих персональные данные с истекшими сроками хранения, рассматривается комиссией Учреждения, состав которой утверждается приказом руководителя Учреждения.

5.6. По итогам заседания комиссии Учреждения составляются протокол и акт о выделении к уничтожению документов, опись уничтожаемых дел. Акт о выделении к уничтожению документов подписывается председателем и членами комиссии и утверждается руководителем Учреждения.

5.7. Уничтожение персональных данных по окончании срока их обработки на электронных носителях производится путем механического нарушения их целостности, не позволяющим произвести считывание и восстановление персональных данных, или удаления с электронных носителей методами и средствами гарантированного удаления остаточной информации.

6. Рассмотрение запросов субъектов персональных данных или их представителей

6.1. Лица, указанные в пункте 2.5., 2.8. настоящей Политики, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных Учреждением;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые Учреждением способы обработки персональных данных;

4) наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным, непосредственно осуществляющим обработку персональных данных;

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

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

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

8) информацию о способах исполнения Учреждением обязанностей, установленных статьей 18.1 Федерального закона «О персональных данных»;

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

6.2. Лица, указанные в пункте 2.5., 2.8. настоящей Политики, вправе требовать от Учреждения уточнения их персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.3. Сведения, указанные в пункте 6.1. настоящей Политики, должны быть предоставлены субъекту персональных данных Учреждением в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.4. 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. Обязанности Учреждения при обработке персональных данных

7.1. Издавать правовые акты по вопросам обработки персональных данных, а также правовые акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации и иных нормативных правовых актов, связанных с обработкой персональных данных, устранение последствий таких нарушений.

7.2. Определять состав и перечень правовых, организационных и технических мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

7.3. Назначать лицо, ответственное за организацию обработки персональных данных в Учреждении, которое, в частности:

получает указания непосредственно от руководителя Учреждения и подотчетно ему;

осуществляет внутренний контроль за соблюдением законодательства Российской Федерации и иных нормативных правовых актов о персональных данных, в том числе требований к защите персональных данных;

обеспечивает доведение до сведения сотрудников положений законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, правовых актов Учреждения по вопросам обработки персональных данных;

организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществляет контроль за приемом и обработкой таких обращений и запросов.

7.3. Обеспечивать выполнение лицами, осуществляющими обработку персональных данных и лицами, имеющими доступ к персональным данным, требований по защите персональных данных, установленных нормативными правовыми актами.

7.4. Обеспечивать конфиденциальность персональных данных, обрабатываемых в структурных подразделениях, кроме общедоступных персональных данных и случаев обезличивания персональных данных, если иное не предусмотрено федеральным законом.

7.5. Принимать меры по обеспечению безопасности персональных данных при их обработке в структурных подразделениях.

7.6. Не допускать обработку и приобщение к личному делу субъекта персональных данных сведений, касающихся состояния здоровья, расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, членства в общественных объединениях или его профсоюзной деятельности, если иное не предусмотрено федеральным законом.

7.7. Обеспечивать уничтожение персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7.8. Выполнять иные требования в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

8. Порядок доступа к персональным данным и их предоставления

8.1. К обработке персональных данных допускаются сотрудники Учреждения, должностными инструкциями которых предусмотрено выполнение обязанностей по обработке персональных данных.

8.2. Предоставление доступа к персональным данным сотрудниками Учреждения осуществляется на основании перечня должностей, которые предусматривают осуществление обработки персональных данных, либо осуществление доступа к персональным данным, утвержденного правовым актом Учреждения, принимаемым в форме приказа.

8.3. При организации доступа сотрудника к персональным данным, он знакомится под роспись с требованиями федерального законодательства и правовых актов Учреждения к обработке персональных данных и обеспечению безопасности персональных данных.

8.4. Лицам, допущенным к обработке персональных данных, предоставляется доступ только к персональным данным, необходимым для выполнения их служебных обязанностей в пределах задач и функций соответствующих структурных подразделений Учреждения.

8.5. Каждое лицо, допущенное к автоматизированной обработке персональных данных, использует индивидуальный идентификатор и пароль, которые не имеет права передавать другим лицам.

8.6. Структурные подразделения Учреждения вправе передавать (распространять, предоставлять, давать доступ) персональные данные третьим лицам с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, либо путем принятия Учреждением правового акта. В правовом акте должны быть определены перечень действий (операций) с персональными данными и цели их обработки, должна быть установлена обязанность лица, которому предоставлены персональные данные, соблюдать конфиденциальность и обеспечивать безопасность персональных данных, а также должны быть указаны требования к их защите в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

8.7. Основанием для отказа в предоставлении персональных данных третьим лицам являются:

8.7.1. Отсутствие согласия субъекта персональных данных.

8.7.2. Отсутствие условий, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», при которых согласие субъекта персональных данных не требуется.

9. Организация защиты персональных данных

9.1. Персональные данные относятся к сведениям ограниченного доступа и подлежат защите в рамках функционирующей в Учреждении системы защиты информации.

9.2. При организации защиты персональных данных при их обработке Учреждение руководствуется, в том числе:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами»;

- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказами ФСТЭК России № 55, ФСБ России № 86, Мининформсвязи России № 20 от 13 февраля 2008 г. «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

- Указом Президента Российской Федерации от 06 марта 1997 г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Трудовым кодексом Российской Федерации.

9.3. Субъектами отношений при организации системы защиты для обеспечения безопасности персональных данных при их обработке в Учреждении (далее – субъекты информационных отношений) являются:

- Учреждение как оператор, осуществляющий обработку персональных данных;

- Сотрудники Учреждения, допущенные к обработке персональных данных, в соответствии с возложенными на них полномочиями и функциями.

9.4. Под безопасностью информации понимают состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

9.5. Задачами системы защиты персональных данных являются исключение или минимизация ущерба от возможной реализации случайных или злонамеренных воздействий на персональные данные, а также прогнозирование и предотвращение таких воздействий.

9.6. Меры, принимаемые для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных, подразделяются на правовые, организационные и технические.

9.6.1. К правовым мерам защиты персональных данных относится принятие правовых актов Учреждением в соответствии с федеральными законами в области защиты

персональных данных и принятыми в их исполнение нормативными документами, закрепляющих права и обязанности субъектов информационных отношений в процессе обработки персональных данных, а также устанавливающих ответственность за нарушение этих правил.

9.6.2. К **организационным мерам** защиты персональных данных относятся, в том числе:

9.6.2.1. Назначение в Учреждении лиц, ответственных за обеспечение безопасности информации.

9.6.2.2. Разработка и поддержание в актуальном состоянии организационно-распорядительных документов, регламентирующих порядок обработки персональных данных, создания и функционирования системы защиты персональных данных.

9.6.2.3. Организация деятельности субъектов информационных отношений, в том числе:

Установление перечня должностей, который предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

Осуществление обработки персональных данных с согласия субъектов персональных данных;

Информирование лиц, осуществляющих обработку персональных данных, о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

Обеспечение отдельной фиксации на материальных носителях персональных данных, имеющих различную цель обработки, или их отдельной обработки;

Обеспечение отдельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

Своевременное устранение выявленных нарушений законодательства об обработке и защите персональных данных.

9.6.2.4. Осуществление внутреннего контроля соответствия обработки и безопасности персональных данных в Администрации Краснодонского сельского поселения требованиям законодательства Российской Федерации и иных нормативных правовых актов о персональных данных, в том числе требованиям к защите персональных данных.

9.6.2.5. Проведение мероприятий по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с персональными данными.

9.6.2.6. Обучение, периодическое повышение квалификации, проведение инструктажей сотрудников, ответственных за организацию обработки и обеспечение безопасности информации, сотрудников, непосредственно выполняющих мероприятия по обеспечению безопасности персональных данных.

9.6.2.7. Осуществление ознакомления сотрудников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе требованиями к защите персональных данных, Политикой и иными внутренними регулятивными документами по вопросам обработки персональных данных.

9.6.2.8. Осуществление хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше чем этого требуют цели обработки персональных данных, если срок хранения не установлен федеральным законом.

9.6.3. К **техническим мерам** защиты относится использование программно-аппаратных средств, выполняющих самостоятельно или в комплексе с другими средствами функции защиты персональных данных, и методов защиты, в том числе:

Программой или программно-технической защиты от несанкционированного доступа к информационным ресурсам автоматизированных рабочих мест, на которых обрабатываются персональные данные;

Программно-технических средств, позволяющих восстанавливать персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;

Средств защиты персональных данных от утечки по техническим каналам при их обработке, хранении и передаче по каналам связи;

Средств межсетевого экранирования при подключении автоматизированных рабочих мест к локальным сетям общего пользования или к сети Интернет;

Криптографических средств защиты информации;

Средств защиты от вредоносного программного обеспечения.

9.7. В Учреждении применяются сертифицированные средства защиты информации, соответствующие требованиям, установленным уполномоченными органами в области технической защиты информации.

9.8. В случае принятия решения о проведении работ по обезличиванию персональных данных разрабатываются правила работы с обезличенными данными в соответствии с приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

9.9. Лицо, ответственное за организацию обработки персональных данных в Учреждении, при обеспечении безопасности персональных данных, в частности, вправе:

иметь доступ к информации, касающейся обработки персональных данных;

привлекать к реализации мер, направленных на обеспечение безопасности персональных данных, обрабатываемых в структурных подразделениях, сотрудников с возложением на них соответствующих обязанностей и закреплением ответственности.

9.10. При обработке персональных данных с использованием средств автоматизации Учреждением, в частности, применяются следующие меры:

9.10.1. Назначается ответственный за организацию обработки персональных данных, из числа сотрудников Учреждения, определяется его компетенция;

9.10.2. Утверждаются внутренние регулятивные документы по вопросам обработки и защиты персональных данных, в том числе устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений;

9.10.3. Осуществляется внутренний контроль (аудит) соответствия обработки персональных данных законодательству о персональных данных и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Политике и внутренним регулятивным документам Учреждения;

9.10.4. Проводится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства о персональных данных, определяется соотношение указанного вреда и принимаемых Учреждением мер, направленных на обеспечение исполнения обязанностей, предусмотренных законодательством о персональных данных.

9.11. Обеспечение безопасности персональных данных в Учреждении, при их обработке в информационных системах персональных данных, достигается в частности путем:

9.11.1. Определения угроз безопасности персональных данных, типа актуальных угроз безопасности персональных данных и необходимого уровня защищенности персональных данных в соответствии с требованиями законодательства и с учетом проведения оценки возможного вреда;

9.11.2. Определения в установленном порядке состава и содержания мер по обеспечению безопасности персональных данных, выбора средств защиты информации. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности Учреждением могут разрабатываться компенсирующие меры, направленные на

нейтрализацию актуальных угроз безопасности персональных данных. В этом случае в ходе разработки системы защиты персональных данных проводится обоснование применения компенсирующих мер для обеспечения безопасности персональных данных;

9.11.3. Применения организационных и технических мер по обеспечению безопасности персональных данных необходимых для выполнения требований к защите персональных данных, обеспечивающих определенные уровни защищенности персональных данных, включая применение средств защиты информации, прошедших процедуру оценки соответствия, когда применение таких средств необходимо для нейтрализации актуальных угроз.

В Учреждении, в том числе, осуществляются:

оценка эффективности принимаемых и реализованных мер по обеспечению безопасности персональных данных;

учет машинных носителей персональных данных, обеспечение их сохранности;

обнаружение фактов несанкционированного доступа к персональным данным и принятие соответствующих мер;

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

установление правил доступа к обрабатываемым персональным данным, а также обеспечение регистрации и учета действий, совершаемых с персональными данными;

организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

контроль за принимаемыми мерами по обеспечению безопасности персональных данных, уровня защищенности информационных систем персональных данных.

9.12. Обеспечение защиты персональных данных в Учреждении при их обработке, осуществляемой без использования средств автоматизации, достигается, в частности, путем:

9.12.1. Обособления персональных данных от иной информации;

9.12.2. Недопущения фиксации на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы;

9.12.3. Использования отдельных материальных носителей для обработки каждой категории персональных данных;

9.12.4. Принятия мер по обеспечению отдельной обработки персональных данных 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;

9.12.5. Соблюдения требований:

к отдельной обработке зафиксированных на одном материальном носителе персональных данных и информации, не относящейся к персональным данным;

уточнению персональных данных;

уничтожению или обезличиванию части персональных данных;

использованию типовых форм документов, характер информации в которых предполагается или допускается включение в них персональных данных;

хранению персональных данных, в том числе к обеспечению отдельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях, и установлению перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

10. Ответственность за нарушение требований законодательства Российской Федерации в области персональных данных

10.1. Ответственный за организацию обработки персональных данных в Учреждении несет ответственность за надлежащее выполнение возложенных функций по организации обработки персональных данных в структурных подразделениях в соответствии с законодательством Российской Федерации и иными нормативными правовыми актами в области персональных данных.

10.2. Лица, осуществляющие обработку персональных данных в структурных подразделениях, в соответствии со своими полномочиями, несут гражданско-правовую, уголовную, административную, дисциплинарную ответственность за нарушение требований к обработке и защите персональных данных, предусмотренную законодательством Российской Федерации.

11. Правовые основания обработки персональных данных

11.1 Политика обработки персональных данных в Учреждении определяется в соответствии со следующими нормативными правовыми актами:

Конституция Российской Федерации;

Трудовой кодекс Российской Федерации;

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

Постановление Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Налоговый кодекс Российской Федерации;

Федеральный закон от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»;

Федеральный закон от 06.12.11 № 402-ФЗ «О бухгалтерском учете»;

Федеральный закон от 17.12.01 № 173-ФЗ «О трудовых пенсиях в Российской Федерации»;

Федеральный закон от 15.12.01 № 167-ФЗ «Об обязательном пенсионном страховании в Российской Федерации»;

Федеральный закон от 24.07.09 № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»;

Бюджетный кодекс Российской Федерации;

Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции»;

Гражданский кодекс Российской Федерации;

Постановление Правительства Российской Федерации от 30 июня 2015 г. № 658 «О государственной интегрированной информационной системе управления общественными финансами «Электронный бюджет» (Собрание законодательства Российской Федерации, 2015, Ха 28, ст. 4228; 2022, Ха 37,6367).

Часть 1 статьи 21 Федерального закона от 27 июля 2010г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Приказ министерства финансов Ростовской области от 30.11.2021 № 233 "О вводе в эксплуатацию системы защиты информации информационной системы «Единая автоматизированная система управления общественными финансами в Ростовской области» и подключения пользователей "

Договоры, заключаемые между оператором и субъектом персональных данных;
Согласия субъектов персональных данных на обработку персональных данных;
Устав Учреждения.

Иные правовые акты и документы, регламентирующие в Учреждении вопросы обработки персональных данных.