Приложение № 1
к приказу директора школы
от 30.12.2020 № 525

ПОЛОЖЕНИЕ
о защите, хранении, обработке и передаче персональных данных в МОУ «СОШ № 39 им. Г.А. Чернова» г. Воркуты

1. Общие положения

Настоящее Положение о защите, хранении, обработке и передаче персональных данных в МОУ «СОШ № 39 им. Г.А. Чернова» г. Воркуты (далее – Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и иными нормативными правовыми актами Российской Федерации.

1.1. Цель разработки настоящего Положения – определение порядка сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения персональных данных, обрабатываемых в МОУ «СОШ №39 им. Г.А. Чернова» г. Воркуты (далее – Учреждение), и установление ответственности должностных лиц Учреждения, непосредственно осуществляющих обработку персональных данных и (или) имеющих доступ к персональным данным.

1.2. Настоящее Положение вступает в силу с момента его утверждения директором Учреждения и действует бессрочно до замены его новым Положением или до наступления иных случаев, предусмотренных законодательством.

1.3. Настоящее Положение является обязательным для исполнения всеми сотрудниками Учреждения, непосредственно осуществляющими обработку персональных данных и (или) имеющими доступ к персональным данным субъектов персональных данных. Все сотрудники Учреждения, непосредственно осуществляющие обработку персональных данных и (или) имеющие доступ к персональным данным, должны быть ознакомлены с настоящим Положением под подпись.

1.4. Настоящее Положение подлежит корректировке при изменении законодательных и нормативно-правовых актов, по рекомендациям надзорных органов, по результатам проверок в рамках государственного контроля (надзора).

1.5. Ответственность за актуализацию настоящего Положения и текущий контроль над выполнением норм настоящего Положения возлагается на ответственного за организацию обработки персональных данных, назначенного приказом Учреждения.

1.6. Учреждение учитывает требования настоящего Положения при разработке и утверждении любых внутренних документов Учреждения, связанных с обработкой персональных данных.

1.7. В настоящем Положении используются следующие понятия, термины и сокращения:

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

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Обработка персональных данных без использования средств автоматизации (неавтоматизированная) – обработка (использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных), содержащихся в информационной системе персональных данных либо извлеченных из такой системы персональных данных, осуществляемая при непосредственном участии человека.

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

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

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.

2. Обработка персональных данных

2.1. Общие требования при обработке персональных данных

2.1.1. Сотрудники Учреждения при обработке персональных данных гражданина Российской Федерации обязаны соблюдать следующие общие требования:

– обработка персональных данных в Учреждении осуществляется в целях выполнения требований трудового законодательства Российской Федерации, оформления договорных отношений в соответствии с законодательством Российской Федерации;

– при определении объема и содержания обрабатываемых персональных данных, сотрудники Учреждения должны руководствоваться Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;

– обработка специальных категорий персональных данных, касающихся состояния здоровья, допускается на основании ст.10 Федерального закона «О персональных данных»;

– Учреждение не обрабатывает биометрические персональные данные. Сканирование фотографий в документах, идентифицирующих личность субъектов персональных данных (например, в паспортах), в Учреждении не осуществляется. Передаваемые в рамках трудового законодательства, а также в рамках договоров, копии паспортов субъектов персональных данных, не используются в целях идентификации личности. В случае если обработка биометрических персональных данных субъекта персональных данных Учреждения необходима по действующему законодательству или для осуществления деятельности Учреждения, то такая обработка осуществляется с письменного согласия субъекта персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации в области персональных данных;

– в целях информационного обеспечения могут создаваться общедоступные источники персональных данных. В общедоступные источники персональных данных с письменного согласия сотрудника могут включаться его фамилия, имя, отчество, должность, номер контактного телефона и иные данные. Сведения о сотруднике Учреждения должны быть в любое время исключены из общедоступных источников персональных данных по запросу сотрудника либо по решению суда или иных уполномоченных государственных органов;

– обработка персональных данных в Учреждении осуществляется только специально уполномоченными лицами, перечень которых утверждается приказом Учреждения, при этом указанные в приказе сотрудники должны иметь право получать только те персональные данные субъекта, которые необходимы для выполнения непосредственных должностных обязанностей;

– сотрудники Учреждения, осуществляющие обработку персональных данных, должны быть проинформированы о факте такой обработки, об особенностях и правилах такой обработки, установленных нормативно-

правовыми актами и внутренними документами Учреждения, об ответственности за разглашение конфиденциальной информации, к которой относится в том числе информация, содержащая персональные данные;

– в рамках информирования сотрудников Учреждения о факте обработки персональных данных, Учреждение обязывает сотрудников соблюдать внутренние нормативные документы, регламентирующие как общий порядок работы с персональных данных, так и специальные нормы, касающиеся совершения отдельных действий, связанных с обработкой персональных данных субъектов персональных данных Учреждения.

2.2. Состав персональных данных и перечень документов на бумажных носителях, содержащих персональные данные

2.2.1. В Учреждении обрабатываются персональные данные следующих субъектов персональных данных:

– работников и учащихся Учреждения;
– граждан, состоящих с Учреждением в гражданско-правовых отношениях.

2.2.2. К персональным данным относятся следующие сведения:

– ФИО;
– дата, место рождения;
– гражданство;
– адрес регистрации, проживания;
– контактные телефоны;
– паспортные данные;
– ИНН;
– СНИЛС;
– серия, номер полиса ОМС;
– сведения об образовании;
– уровень владения иностранными языками;
– характер, вид работы;
– табельный номер;
– подразделение;
– профессия, должность
– специальность, категория;
– стаж работы;
– состояние в браке;
– сведения о составе семьи;
– сведения о воинском учете;
– сведения о приеме на работу и переводах на другие должности;
– информация об аттестации;
– информация о квалификации, о повышении квалификации;
– сведения о профессиональной переподготовке;
– информация о наградах (поощрениях), почетных званиях;

– данные об отпусках;
– данные о командировках;
– сведения о социальных льготах, на которые сотрудник имеет право в соответствии с законодательством;
– сведения о доходах;
– сведения о налогах;
– сведения о страховых взносах;
– данные о нетрудоспособности;
– фотография;
– номер банковского счета;
– прочие сведения, с помощью которых можно идентифицировать субъекта персональных данных.

2.2.3. К документам (в бумажном и (или) электронном виде), содержащим персональные данные работников Учреждения, относятся:

– Документы, необходимые для расчета и начисления заработной платы и иных выплат сотрудникам (табель учета использования рабочего времени, карточка-справка, заявления, расчетные ведомости по начислению заработной платы работникам, документы о выплате пособий, оплате листков нетрудоспособности, командировочное удостоверение и др.);
– Документы, необходимые для ведения расчетно-кассовой деятельности (расходно-кассовый ордер, платежные поручения, счета на оплату и др.);
– Документы, необходимые для расчета с Федеральной налоговой службой и различными фондами (регистр налогового учета, листок нетрудоспособности, сведения о сумме выплат и иных вознаграждений, о начисленных и уплаченных страховых взносах на обязательное пенсионное страхование и страховом стаже застрахованного лица и др.);
– Справки (по форме 2-НДФЛ, 6-НДФЛ, о зарплате, с места работы и др.);
– Договоры о материальной ответственности;
– Личные дела сотрудников (личный листок по учету кадров, резюме, заявление о приеме на работу, трудовой договор, протоколы по определению стажа работы, ксерокопии документов и др.);
– Личные карточки сотрудников (ф. № Т-2);
– Приказы по личному составу (о приеме, увольнении, смене фамилий, премировании, доплатах, надбавках);
– Приказы о предоставлении отпусков, командировках, взысканиях;
– Трудовые договоры (в т.ч. срочные), дополнительные соглашения к ним, не вошедшие в состав личных дел;
– Графики отпусков;
– Заявления работников, не вошедшие в состав личных дел;
– Трудовые книжки;
– Справки;
– Документы о награждении (представления, характеристики, списки);

– Документы по аттестации (протоколы, анкеты, характеристики, переписка, планы);
– Списки работников;
– Документы по воинскому учету граждан;
– Книги учета по вопросам кадрового учета;
– Журналы регистрации по вопросам кадрового учета.

2.2.4. К общедоступным персональным данным работников Учреждения относятся следующие сведения:

– ФИО;
– должность;
– место работы;
– специальность и квалификационная категория;
– образование;
– наименование ВУЗа;
– год получения диплома;
– сведения о наградах;
– звания;
– фотография.

2.2.5. К персональным данным граждан, состоящих с Учреждением в гражданско-правовых отношениях, относятся следующие сведения:

– ФИО;
– адрес;
– паспортные данные;
– ИНН;
– номер расчетного счета.

2.2.6. К документам (в бумажном и (или) электронном виде), содержащим персональные данные сотрудников Учреждения, относятся:

- личные дела сотрудников и учащихся;
- журналы приказов по основной деятельности, по личному составу и по кадрам.

2.3. Получение персональных данных

2.3.1. Все персональные данные следует получать непосредственно от субъекта персональных данных. Субъект самостоятельно принимает решение о предоставлении своих персональных данных, и дает согласие на их обработку Учреждением. В случае если Учреждение получает персональные данные субъектов персональных данных от третьих лиц, получающих персональные данные у субъектов, в соответствие с ч. 4 ст. 6 Федерального закона «О персональных данных», Учреждение не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

2.3.2. Если персональные данные получены не от субъекта персональных данных и их обработка не поручена Учреждению, Учреждение до начала обработки таких персональных данных обязано предоставить субъекту

персональных данных следующую информацию: наименование либо фамилия, имя, отчество и адрес оператора или его представителя; цель обработки персональных данных и ее правовое основание; предполагаемые пользователи персональных данных; установленные Федеральным законом «О персональных данных» права субъекта персональных данных; источник получения персональных данных.

2.3.3. Учреждение освобождается от обязанности предоставить субъекту персональных данных указанные сведения в случаях, если:

– субъект персональных данных Учреждения уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

– персональные данные получены Учреждением на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных Учреждения;

– персональные данные сделаны общедоступными субъектом персональных данных Учреждения или получены из общедоступного источника;

– Учреждение осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных Учреждения.

2.3.4. Обработка персональных субъектов персональных данных Учреждения осуществляется с их согласия на обработку их персональных данных, а также в иных случаях, предусмотренных ст. 6 Федерального закона «О персональных данных». Согласие на обработку персональных данных может быть дано субъектом персональных данных или его законным представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных, полномочия данного представителя проверяются Учреждением. Форма согласия может быть в письменной или иной форме, предусмотренной действующим законодательством. При недееспособности субъекта персональных данных письменное согласие на обработку его данных дает его законный представитель. Учреждение обязано иметь доказательство получения согласия субъекта персональных данных на обработку его персональных данных (в том случае, если такое согласие является необходимым).

2.3.5. В случаях, предусмотренных ч. 4 ст. 9 Федерального закона «О персональных данных», обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Письменное согласие субъекта на обработку его персональных данных должно включать в себя:

– фамилию, имя, отчество, адрес субъекта, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

– фамилию, имя отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

– адрес Учреждения;

– цель обработки персональных данных;

– перечень персональных данных, на обработку которых дается согласие субъекта;

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

– перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки персональных данных;

– срок, в течение которого действует согласие, а также порядок его отзыва;

– подпись субъекта персональных данных.

2.3.6. В соответствии с п.5 ч.1 ст. 6 Федерального закона «О персональных данных» для осуществления обработки персональных данных работников Учреждению не требуется получать согласие субъектов на обработку их данных. Исключение составляет согласие на поручение обработки персональных данных третьим лицам, передачу персональных данных третьим лицам, если такая передача не предусмотрена законодательством, и согласие считать определенные персональные данные общедоступными.

2.3.7. В соответствии с п.5 ч.1 ст. 6 Федерального закона «О персональных данных» для осуществления обработки персональных данных граждан, состоящих с Учреждением в гражданско-правовых отношениях, Учреждению не требуется получать согласие субъектов на обработку их данных. Исключение составляет согласие на поручение обработки персональных данных третьим лицам.

2.3.8. Передача персональных данных субъектов персональных данных Учреждения третьим лицам (включая надзорные, правоохранительные органы) возможна только в случаях, прямо предусмотренных законодательными и нормативными актами, либо в случае согласия субъекта персональных данных. В случае если обязанность либо возможность предоставления имеющихся в распоряжении Учреждения персональных данных иным лицам (включая органы государственной и муниципальной власти) установлена законодательством, Учреждение обязано предоставить указанные данные в составе, виде и сроки, указанные в законодательных или нормативных актах. Если обязанность предоставления персональных данных фиксируется соответствующим запросом (ходатайством) уполномоченного лица, запрос подлежит обязательной проверке в целях контроля над обоснованностью предоставления запроса. При

обоснованности подобного запроса Учреждение формирует ответ на запрос. При необоснованности запроса Учреждение направляет отправителю запроса письменное уведомление об отказе в предоставлении персональных данных. При передаче персональных данных третьим лицам Учреждение обязано уведомлять лиц, получивших персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные, обязаны соблюдать их конфиденциальность и безопасность. Данное требование не распространяется на обмен персональными данными в порядке, установленном законодательством.

2.3.9. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных при условии, что подобная процедура не нарушает требований законодательства Российской Федерации. В случае отзыва субъектом персональных данных Учреждения согласия на обработку персональных данных Учреждение вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пп. 2-11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст. 11 Федерального закона «О персональных данных».

2.3.10. В соответствии с пп. 2-11 ч. 1 ст. 6, ч. 4 ст. 6, ч.2 ст. 10 и ч. 2 ст. 11 Федерального закона «О персональных данных» обработка персональных данных может осуществляться без согласия субъекта персональных данных.

2.3.11. Трансграничная передача персональных данных в Учреждении не осуществляется.

2.4. Порядок обработки персональных данных с использованием средств автоматизации и без использования средств автоматизации

2.4.1. Обработка персональных данных в Учреждении может проводиться с использованием средств автоматизации (информационных систем) и без таковых. Конкретный способ обработки персональных данных определяется на основании процедур использования данных, определенных внутренними документами Учреждения.

2.4.2. Перечень информационных систем, в которых обрабатываются персональные данные, уровень защищенности персональных данных при их обработке в информационных системах персональных данных, требования по обеспечению безопасности обрабатываемых в них персональных данных субъектов персональных данных Учреждения описаны в отдельных нормативных актах Учреждения.

2.4.3. Контроль за соответствием обработки персональных данных заявленным целям возлагается на ответственного за организацию обработки персональных данных в Учреждении, и на руководителей подразделений, в которых осуществляется обработка персональных данных.

2.4.4. Исключительно автоматизированная обработка персональных данных в Учреждении не осуществляется. Во всех процессах обработки персональных

данных субъектов персональных данных с использованием средств автоматизации принимают участие ответственные сотрудники Учреждения.

2.4.5. Обработка персональных данных без использования средств автоматизации (далее – неавтоматизированная обработка персональных данных) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

2.4.6. При неавтоматизированной обработке персональных данных на бумажных носителях:

– не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;

– персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

– документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

– дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

2.4.7. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

2.4.8. 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).

2.5. Доступ к персональным данным

2.5.1. Перечень должностей сотрудников Учреждения, осуществляющих обработку персональных данных, как в бумажном, так и в электронном виде и (или) имеющих доступ к персональным данным, утверждается приказом Учреждения. При этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения непосредственных должностных обязанностей.

2.5.2. В случае если Учреждению оказывают услуги юридические и физические лица на основании заключенных договоров (либо иных оснований) и в силу данных договоров они должны иметь доступ к персональным данным субъектов персональных данных Учреждения, то соответствующие данные предоставляются Учреждением только после подписания с лицами, осуществляющими обработку персональных данных по поручению Учреждения, соответствующего соглашения, в котором должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки,

должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со ст. 19 Федерального закона «О персональных данных».

2.5.3. Процедура оформления доступа к персональным данным включает в себя:

– ознакомление сотрудников с настоящим Положением, инструкцией пользователя информационных систем персональных данных и другими нормативными актами, регулирующими обработку и защиту персональных данных в Учреждении, под роспись;

– подписание сотрудником Учреждения обязательства о соблюдении конфиденциальности персональных данных.

2.6. Обеспечение конфиденциальности персональных данных

2.6.1. Персональные данные относятся к категории конфиденциальной информации.

2.6.2. Учреждение вправе поручить обработку персональных данных другим юридическим или физическим лицам на основании договора (далее – поручение Учреждения) с согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом «О персональных данных». Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом «О персональных данных». В поручении Учреждения должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

2.6.3. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных. В случае если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

2.6.4. Необходимость доступа сотрудников Учреждения к персональным данным субъектов персональных данных, обрабатываемым в Учреждении, должна быть документально определена в соответствующих должностных инструкциях.

2.6.5. Обработка и защита персональных данных в структурных подразделениях Учреждения осуществляется в документально определенном порядке, исключающем несанкционированный доступ к персональным данным.

2.6.6. В Учреждении документально определен перечень лиц, осуществляющих обработку персональных данных. Лица, осуществляющие такую обработку, проинформированы о факте обработки ими персональных данных, об особенностях и правилах осуществления такой обработки, а также об ответственности за нарушение действующего законодательства в области персональных данных. Лица, осуществляющие обработку персональных данных, ознакомлены под роспись с настоящим Положением и подписали обязательство о соблюдении конфиденциальности персональных данных и соблюдении правил обработки персональных данных.

2.6.7. В Учреждении документально определен перечень помещений, в которых ведется обработка персональных данных, порядок доступа сотрудников в вышеуказанные помещения.

2.6.8. Передача персональных данных между структурными и территориальными подразделениями Учреждения осуществляется только между сотрудниками, включенными в перечень лиц, имеющих доступ к персональным данным.

2.6.9. Сотрудники Учреждения и иные лица, получающие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством в сфере защиты персональных данных.

2.7. Права и обязанности сторон при обработке персональных данных

2.7.1. Субъекты персональных данных обязаны предоставлять Учреждению только достоверные, документированные персональные данные.

2.7.2. Каждый субъект персональных данных имеет право:

– на получение полной информации о своих персональных данных и на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных ч.8 ст.14 Федерального закона «О персональных данных»;

– на получение информации, касающейся обработки его персональных данных, в том числе содержащей: подтверждение факта обработки, правовые основания и цель обработки; способы обработки, наименование и место нахождения Учреждения, сведения о лицах, которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением или на основании Федерального закона «О персональных данных»; обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом «О персональных данных»; сроки обработки персональных данных, в

том числе сроки их хранения; порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»; наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения, если обработка поручена или будет поручена такому лицу; иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами. Сведения, указанные выше, предоставляются субъекту персональных данных или его представителю оператором при обращении либо при получении запроса субъекта персональных данных или его уполномоченного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его уполномоченного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением, подпись субъекта персональных данных или его уполномоченного представителя;

– обратиться повторно в Учреждение или направить повторный запрос в целях получения сведений, указанных выше, и ознакомления с такими персональными данными не ранее чем через 30 (тридцать) дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения;

– требовать от сотрудников Учреждения уточнения своих 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;

– заявить о своем несогласии при отказе сотрудников Учреждения исключить или исправить персональные данные (в письменной форме с соответствующим обоснованием такого несогласия).

2.7.3. Учреждение обязано безвозмездно предоставить субъекту персональных данных возможность ознакомления с персональными данными, относящимися к этому субъекту, а также внести в них необходимые изменения при предоставлении субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными.

2.7.4. Учреждение обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую

информацию в течение 30 (тридцати) календарных дней с даты получения такого запроса.

2.8. Передача персональных данных

2.8.1. При передаче персональных данных субъекта сотрудники Учреждения обязаны соблюдать следующие требования:

– не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, предусмотренных Гражданским Кодексом Российской Федерации или иными федеральными законами;

– предупреждать лица, получающие персональные данные субъектов, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц обеспечения конфиденциальности полученных персональных данных;

– не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;

– передавать персональные данные субъекта представителям субъектов в порядке, установленном Гражданским Кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функций;

– не отвечать на вопросы, связанные с передачей персональных данных субъекта по телефону или факсу, за исключением случаев, связанных с выполнением соответствующими сотрудниками своих непосредственных должностных обязанностей, адресатам в чью компетенцию входит получение такой информации.

2.9. Хранение персональных данных

2.9.1. Хранение персональных данных должно осуществляться 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. Обрабатываемые персональные данные подлежат уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом. Хранение персональных данных в Учреждении может осуществляться на бумажных и машинных носителях, доступ к которым ограничен списком лиц, допущенных к обработке персональных данных.

2.9.2. Все хранимые или используемые средства защиты информации (далее - СЗИ), эксплуатационная и техническая документация к ним подлежат поэкземплярному учету и выдаются под подпись в Журнале поэкземплярного учета СЗИ, эксплуатационной и технической документации к ним пользователям СЗИ, несущим персональную ответственность за их сохранность.

2.9.3. Все хранимые или используемые криптосредства (средства криптографической защиты информации), эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету и выдаются под подпись в Журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов ответственным пользователем криптосредств пользователям криптосредств, несущим персональную ответственность за их сохранность.

2.9.4. Хранение персональных данных субъектов должно происходить в порядке, исключающем их утрату или их неправомерное использование.

2.9.5. Персональные данные субъектов, содержащиеся на бумажных носителях и отчуждаемых машинных носителях информации, должны храниться в сейфах или запираемых шкафах, установленных в пределах контролируемых зон Учреждения, утвержденных приказом Учреждения.

2.9.6. Персональные данные субъектов, содержащиеся на машинных носителях информации могут храниться на автоматизированных рабочих местах и серверах информационных систем персональных данных Учреждения, установленных в пределах контролируемых зон Учреждения.

2.10. Архивирование и обезличивание персональных данных

2.10.1. Персональные данные, не используемые в операционной деятельности Учреждения и цель обработки которых не достигнута, могут быть переведены на архивное хранение с соблюдением всех необходимых требований, предусмотренных Федеральным законом от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации» и иными нормативными актами в сфере организации хранения, комплектования, учета и использования архивных документов независимо от их форм собственности.

2.10.2. Архивирование персональных данных производится в рамках действующих в Учреждении систем документооборота и работы с архивными документами с соблюдением принципов, изложенных в настоящем Положении. Обязательным условием архивирования персональных данных является обеспечение их конфиденциальности и безопасности.

2.10.3. Подразделения Учреждения, хранящие архивные персональные данные на бумажных носителях, обязаны обеспечить ограничение доступа к указанным данным только тех сотрудников, деятельность которых непосредственно связана с обработкой хранимого типа архивных персональных данных. Доступ к архивным персональным данным, хранение которых осуществляется на электронных носителях, должен быть ограничен исходя из требований информационной безопасности, указанных в данном Положении и отдельных локальных нормативных актах Учреждения.

2.10.4. С целью уменьшения объема персональных данных, подлежащих защите в соответствие с требованиями Федерального закона «О персональных данных», подзаконных актов и методических указаний, а также в целях снижения нагрузки и обременений на Учреждение, приводящих к дополнительным затратам без повышения уровня защищенности персональных данных и прав субъектов

персональных данных Учреждения, может быть произведено обезличивание персональных данных субъектов персональных данных Учреждения. Также обезличивание производится в целях предоставления статистической отчетности, агрегированной информации о деятельности Учреждения, а также в иных целях, предусмотренных действующим законодательством, например, по достижении целей их обработки или в случае утраты необходимости в достижении этих целей в соответствии со ст. 5 Федерального закона «О персональных данных».

2.10.5. Обезличенные персональные данные должны представлять собой информацию на бумажном или магнитном носителе, принадлежность которой к конкретному физическому лицу невозможно определить без использования дополнительной информации в силу произведенных при обработке персональных данных действий.

2.10.6. Решение о необходимости и способе обезличивания персональных данных принимает ответственный за организацию обработки персональных данных в Учреждении.

2.11. Прекращение обработки и уничтожение персональных данных

2.11.1. Уничтожение персональных данных субъектов производится Учреждением:

– при выявлении неустранимых неправомерных действий с персональными данными;

– по достижении целей обработки персональных данных (при условии невозможности обезличивания персональных данных);

– при получении от субъекта персональных данных отзыва согласия на обработку персональных данных (при условии, что такой отзыв не противоречит обязанностям Учреждения продолжать обработку персональных данных в соответствии с действующим законодательством);

– по требованию субъекта персональных данных или уполномоченного органа по защите прав субъектов персональных данных – если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

2.11.2. Уничтожению подлежат все требуемые к уничтожению персональные данные, зафиксированные на материальных носителях или хранящихся в информационных системах. Уничтожение персональных данных в информационных системах производится должностным лицом, использовавшим указанные данные. Ответственный за организацию обработки персональных данных, контролирует полноту уничтожения указанных данных в информационных системах Учреждения.

2.11.3. Если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения, то Учреждение обязано обеспечить их уничтожение в соответствии с данным Положением.

2.11.4. Решение об уничтожении персональных данных принимается руководителем подразделения, ответственного за обработку соответствующих персональных данных, признанных необходимыми к уничтожению. Решение об

уничтожении должно быть принято в срок, не превышающий 3 (трех) рабочих дней с даты появления оснований к уничтожению персональных данных. После принятия решения об уничтожении руководитель подразделения, ответственного за обработку персональных данных, обязан уведомить об этом ответственного за организацию обработки персональных данных в Учреждении, который назначает комиссию по уничтожению персональных данных.

2.11.5. Уничтожение персональных данных производится руководителем подразделения (для данных, хранящихся в электронной форме) либо комиссией по уничтожению персональных данных (для документов на материальных носителях) в срок не превышающий 10 (десяти) рабочих дней с даты выявления неустранимых неправомерных действий с персональными данными, не превышающий 30 (тридцати) календарных 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 Федеральным законом «О персональных данных» или другими федеральными законами, в срок, не превышающий 30 (тридцати) календарных дней с даты поступления от субъекта персональных данных отзыва согласия на обработку его 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 Федеральным законом «О персональных данных» или другими федеральными законами. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного выше, Учреждение осуществляет уничтожение или обеспечивает уничтожение персональных данных в срок не более чем 6 (шесть) месяцев, если иной срок не установлен федеральными законами.

2.11.6. В случае если, согласно имеющейся у Учреждения информации, персональные данные субъектов персональных данных были направлены третьим лицам, руководитель подразделения, ответственного за обработку соответствующих персональных данных, обязан потребовать у указанных третьих лиц в письменной форме уничтожения персональных данных с изложением оснований для подобного уничтожения.

2.11.7. При необходимости уничтожения персональных данных, являющихся частью материального носителя, содержащего персональные данные, не подлежащие уничтожению, комиссией по уничтожению персональных данных осуществляется вымарывание либо иное физическое удаление данных с условием сохранения данных, не подлежащих уничтожению. Скорректированные подобным образом документы подлежат возврату в соответствующее подразделение.

2.11.8. После уничтожения данных председатель комиссии по уничтожению персональных данных обязан уведомить о данной операции подразделение, передавшее информацию на уничтожение.

2.11.9. Ответственный за организацию обработки персональных данных в Учреждении в рамках проверок по направлениям деятельности контролирует своевременность и полноту уничтожения персональных данных руководителями подразделений.

3. Защита персональных данных

3.1. Учреждение при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие 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.

3.2. Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, используемых в процессе деятельности Учреждения.

3.3. Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

– применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

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

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

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

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3.4. Основными организационными мерами по защите персональных данных в Учреждении являются:

– определение состава сотрудников, функциональные обязанности которых требуют обработки персональных данных;

– обеспечение ознакомления сотрудников с требованиями нормативных актов Учреждения по защите информации;

– обеспечение наличия необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

– организация процесса уничтожения информации;

– организация разъяснительной работы с сотрудниками Учреждения по предупреждению утраты и утечки сведений при работе с конфиденциальными документами, содержащими персональные данные;

– разработка комплекта организационно-распорядительных документов Учреждения, регламентирующих процессы обработки персональных данных.

3.5. В качестве технических мер защиты персональных данных в Учреждении должны применяться:

– антивирусная защита;

– межсетевые экраны;

– специализированные средства защиты информации от несанкционированного доступа.

3.6. После установки (обновления) программного обеспечения ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных должен произвести требуемые настройки средств управления доступом к компонентам персональных электронных вычислительных машин (далее – ПЭВМ) и проверить работоспособность программного обеспечения и правильность его настройки и произвести соответствующую запись в Журнале учета нештатных ситуаций ПЭВМ, выполнения профилактических работ, установки и модификации программных средств ПЭВМ.

3.7. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных должен проводить периодическое тестирование технических и программных средств защиты и вносить результаты в Журнал периодического тестирования средств защиты информации, а также производить проверку электронных журналов.

4. Взаимодействие с контрольно-надзорными органами

4.1. При поступлении запроса от уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) Учреждение обязано сообщить информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати рабочих дней с даты получения такого запроса.

4.2. В случае выявления неправомерной обработки персональных данных по запросу уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента получения указанного запроса на период проверки. В случае выявления неточных персональных данных по запросу уполномоченного органа по защите прав субъектов персональных данных Учреждение обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) с момента получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

4.3. В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных уполномоченным органом по защите прав субъектов персональных данных, обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

4.4. При проведении контрольно-надзорных мероприятий за выполнением требований к обеспечению безопасности персональных данных при их обработке в государственных информационных системах персональных данных, а также в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности и не являющихся государственными информационными системами персональных данных (по решению Правительства Российской Федерации с учетом значимости и содержания обрабатываемых персональных данных), осуществляемых федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности (ФСБ России) и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации (ФСТЭК России), представители вышеуказанных контрольно-надзорных органов не имеют права на ознакомление с персональными данными, обрабатываемыми в информационных системах персональных данных.

4.5. При проведении контрольно-надзорных мероприятий за выполнением требований к обеспечению безопасности персональных данных Учреждение обязано предоставить Журнал учета проверок юридического лица, индивидуального предпринимателя, проводимых органами государственного контроля (надзора), органами муниципального контроля.

4.6. При проведении контрольно-надзорных мероприятий в отношении Учреждения контрольно-надзорными органами, не осуществляющими контроль и надзор в сфере обработки персональных данных, представители вышеуказанных контрольно-надзорных органов имеют право на доступ к персональным данным только в сфере своей компетенции и в пределах своих полномочий в соответствии с законодательством Российской Федерации.

5. Ответственность за разглашение конфиденциальной информации, содержащей персональные данные

5.1. Каждый сотрудник Учреждения, получающий доступ к информации, содержащей персональные данные, несет персональную ответственность за сохранность конфиденциальности информации.

5.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, обрабатываемых Учреждением, несут ответственность в порядке, установленном федеральными законами и полную материальную ответственность в случае причинения их действиями ущерба в соответствии с п.7 ст. 243 Трудового кодекса Российской Федерации.