УТВЕРЖДЕНО:
Заведующий
МБДОУ «Детский сад № 49«Радуга»
приказ № 195-од от 25.12.2020 года.

ПОЛОЖЕНИЕ
об обработке и защите персональных данных работников и участников образовательного процесса МБДОУ «Детский сад № 49 «Радуга»

1. Общие положения

1.1. Настоящее Положение «Об обработке и защите персональных данных работников и участников образовательного процесса МБДОУ «Детский сад № 49 «Радуга» (далее по тексту - Положение) устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным работников и участников образовательного процесса МБДОУ «Детский сад № 49 «Радуга».
1.2. Цель настоящего Положения - защита персональных данных работников от несанкционированного доступа и разглашения, развитие комплекса мер, направленных на обеспечение защиты персональных данных, хранящихся у Работодателя, посредством планомерных действий по совершенствованию организации труда.
1.3. Настоящее Положение разработано на основании Конституции Российской Федерации, ст. 88 Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006г. № 152-ФЗ «О персональных данных», Постановления правительства Российской Федерации от 17.11.2007г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» (в редакции от 23.07.2013 № 205-ФЗ),, Постановления правительства Российской Федерации от 15.12.2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России, и Рособрнадзора с целью уважения прав и основных свобод каждого работника и обучающегося при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.
1.4. Настоящее Положение и изменения к нему утверждаются руководителем и вводятся в действие приказом. Все работники должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

2. Понятие и состав персональных данных

2.1. В настоящем Положении используются следующие понятия и состав персональных данных:
- персональные данные
- любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми и распорядительными документами Минобрнауки России, Рособразования и Рособрнадзора, Положением об обработке и защите персональных данных и приказами организаций - обработка персональных данных
- действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- информационная система персональных данных

- информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- обработка персональных данных без использования средств автоматизации (неавтоматизированная)
- обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
Субъекты персональных данных:
Работники - лица, заключившие трудовой договор с Учреждением;
Обучающиеся - лица, осваивающие основные образовательные программы в настоящее время;
Выпускники - лица, завершившие обучение по основным образовательным программам и получившие документ об образовании.
Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.
2.2. Оператором персональных данных являются образовательные организации и Управление образования. Допускается привлекать для обработки персональных данных уполномоченные организации на основе соответствующих договоров и соглашений.
2.3. Настоящее Положение и изменения к нему утверждаются приказом руководителя. Все работники и обучающиеся должны быть ознакомлены с Положением и изменениями к нему.
2.4.Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.
2.5.К персональным данным работника относятся:
- все биографические сведения;
- образование;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- характер взаимоотношений в семье;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки работников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;,
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

- фотографии;
- и т.п.

Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

2.6. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

2.7.Собственником информационных ресурсов (персональных данных) - является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал работником) или изъявил желание вступить в трудовые отношения с Работодателем.

2.8.Субъект персональных данных самостоятельно решает вопрос передачи Работодателю своих персональных данных.

2.9.Держателем персональных данных является Работодатель, которому работник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством Российской Федерации.

2.10.Права и обязанности Работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным Работодателем - специалистом по кадрам. Сведения о персональных данных работников он может делегировать руководителям структурных подразделений, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

2.11.Потребителями (пользователями) персональных данных работников являются юридические и физические лица, обращающиеся к Работодателю за получением необходимых сведений и пользующиеся ими без права передачи, разглашения.

3. Порядок получения персональных данных

3.1. Получение персональных данных осуществляется в соответствии с нормативно-правовыми актами Российской Федерации в области трудовых отношений и образования, нормативными и распорядительными документами Минобрнауки России и Рособрнадзора, Положением об обработке и защите персональных данных и приказами учреждения на основе согласия субъектов на обработку их персональных данных.

3.2. Оператор не вправе требовать от субъекта персональных данных предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и о его частной жизни.

3.3. Без согласия субъектов осуществляется обработка общедоступных персональных данных или содержащих только фамилии, имена и отчества, обращений и запросов организаций и физических лиц, регистрация и отправка корреспонденции почтовой связью, персональных данных для исполнения трудовых договоров или без использования средств автоматизации, и в иных случаях, предусмотренных законодательством Российской Федерации.

3.4. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами персональных данных, а также в случаях, предусмотренных нормативно-правовыми актами Российской Федерации.

3.5. Обработка персональных данных обучающегося осуществляется для обеспечения соблюдения законов и иных нормативных правовых актов в целях воспитания и обучения обучающегося, обеспечения его личной безопасности, контроля качества образования, пользования льготами, предусмотренными законодательством Российской Федерации и локальными актами администрации.

3.6. Сбор и обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе,

обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
3.7. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
3.8. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации:
- при отсутствии установленных и настроенных сертифицированных средств защиты информации;
- при отсутствии утвержденных организационных документов о порядке эксплуатации информационной системы персональных данных.
3.9. 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 банных) на электронных носителях информации.
3.10. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.
3.11. 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.
3.12. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:
а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;
в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.
3.13. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.

3.14. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.
3.15. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных, составленном по форме согласно приложению к настоящему Положению. К каждому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.
3.16. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:
а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.
3.17. 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.
3.18. 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).
3.19. Персональные данные могут храниться в бумажном и (или) электронном виде централизованно или в соответствующих структурных подразделениях с соблюдением предусмотренных нормативно-правовыми актами Российской Федерации мер по защите персональных данных.
3.20. Право на обработку персональных данных предоставляется работникам структурных подразделений и (или) должностным лицам, определенным Положением об обработке и защите персональных данных, распорядительными документами и иными письменными указаниями Оператора.
3.21. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными регламентами и инструкциями Оператора.
3.22. Право доступа к персональным данным обучающегося имеют: руководители организаций и их заместители (в рамках своих должностных обязанностей); инспектор по кадрам; классные руководители (только к персональным данным обучающегося своей группы); учителя (только к персональным данным обучающегося своего класса); бухгалтера; программист; обучающийся, носитель данных.

3.23. Право доступа к персональным данным работника имеют: руководитель организации; заместители (в рамках своих должностных обязанностей); инспектор по кадрам; бухгалтер; программист; работник, носитель данных. По письменному заявлению работодатель обязан в срок не позднее трех дней со дня подачи заявления выдать ему копии документов, связанных с его работой (копии приказа о приеме на работу, приказов о переводах на другую работу, приказа об увольнении с работы; выписки из трудовой книжки, справки о заработной плате, периоде работы у данного работодателя и др.). Копии документов, связанных с работой, должны быть заверены надлежащим образом и предоставляться работнику безвозмездно.
3.24. Доступ к персональным данным работника вне организаций имеют:
- Государственные органы в соответствии с направлениями их деятельности:
- Департамент образования области;
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.
- Другие организации (сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации с приложением копии заявления работника).
- Родственники и члены семей (персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника).
3.25. При передаче данных лица, имеющие право доступа к персональным данным работника или обучающегося обязаны:
- предупредить лиц, получающих данную информацию о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;
- потребовать от этих лиц письменное подтверждение соблюдения этого условия.
3.26. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных работника или обучающегося, определяются трудовыми договорами и должностными инструкциями.
3.27. Все сведения о передаче персональных данных обучающихся регистрируются в Журнале учета персональных данных, в целях контроля правомерности использования данной информации лицами, ее получившими.
3.28. Все сведения о передаче персональных данных работников регистрируются в Журнале учета персональных данных работников организаций, в целях контроля правомерности использования данной информации лицами, ее получившими.

4. Принципы обработки персональных данных

4.1. Обработка персональных данных работников включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.
4.2. Получение, хранение, комбинирование, передача или любое другое использование персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
4.3.Все персональные данные работника получаются у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах

получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
4.4.Не допускается получение и обработка персональных данных работника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.
4.5.При принятии решений относительно работника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.
4.6.В случаях, непосредственно связанных с вопросами трудовых отношений, возможно получение и обработка данных о частной жизни работника только с его письменного согласия.
4.7.Защита персональных данных работников от неправомерного их использования или утраты обеспечивается Работодателем за счет его средств.
4.8. Пакет анкетно - биографических и характеризующих материалов (далее пакет) работника формируется после издания приказа о его приеме на работу.
4.9. Пакет обязательно содержит личную карточку формы Т2, а также может содержать документы, содержащие персональные данные работника, в порядке, отражающем процесс приема на работу:
-заявление о приеме на работу;
-анкета;
-характеристика-рекомендация;
-результат медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- копия приказа о приеме на работу;
- расписка работника об ознакомлении с документами организации, устанавливающими порядок обработки персональных данных работников, а также об его правах и обязанностях в этой области.
4.10. Анкета является документом пакета, представляющим собой перечень вопросов о биографических данных работника, его образовании, выполняемой работе с начала трудовой деятельности, семейном положении, месте прописки или проживания и т.п. Анкета заполняется работником самостоятельно при оформлении приема на работу. При заполнении анкеты работник должен заполнять все ее графы, на все вопросы давать полные ответы, не допускать исправлений или зачеркивания, прочерков, помарок, в строгом соответствии с записями, которые содержатся в его личных документах. В графе "Ближайшие родственники" перечисляются все члены семьи работника с указанием степени родства (отец, мать, муж, жена, сын, дочь, родные брат и сестра); далее перечисляются близкие родственники, проживающие совместно с работником. Указываются фамилия, имя, отчество и дата рождения каждого члена семьи.
4.11. При заполнении анкеты и личной карточки Т2 используются следующие документы: паспорт; трудовая книжка; военный билет; документы об образовании; документы о присвоении ученой степени, ученого звания. Пакет пополняется на протяжении всей трудовой деятельности работника. Изменения, вносимые в карточку Т2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).
4.12. Специалист по кадрам, ответственный за документационное обеспечение кадровой деятельности, принимает от работника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.
4.12.Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

4.13.При обработке персональных данных работников Работодатель вправе определять способы обработки, документирования, хранения и защиты персональных данных работников на базе современных информационных технологий.
4.14. Обработка полученных в установленных законодательством Российской Федерации случаях персональных данных осуществляется органами прокуратуры в связи с осуществлением ими прокурорского надзора.

5. Права и обязанности работника в целях обеспечения защиты персональных данных

5.1. Работник обязан:
- передавать Работодателю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации;
- своевременно сообщать Работодателю об изменении своих персональных данных.
5.2. Работники имеют право на:
-полную информацию о своих персональных данных и обработке этих данных;
-свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации;
-определение своих представителей для защиты своих персональных данных;
-доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по своему выбору;
-требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона.
При отказе Работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме Работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
-требование об извещении Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях.
- обжалование в суде любых неправомерных действий или бездействий Работодателя при обработке и защите его персональных данных;

6. Права и обязанности оператора персональных данных

6.1. Обязанности оператора при сборе персональных данных:
1. При сборе персональных данных оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона.
2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.
3. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением случаев, предусмотренных частью 4 статьи Федерального закона, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:
1) наименование либо фамилия, имя, отчество и адрес оператора или его представителя;
2) цель обработки персональных данных и ее правовое основание;
3) предполагаемые пользователи персональных данных;
4) установленные настоящим Федеральным законом права субъекта персональных данных;
5) источник получения персональных данных.

4. Оператор освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные частью 3 статьи Федерального закона, в случаях, если:
1) субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;
2) персональные данные получены оператором на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;
3) персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;
4) оператор осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных;
5) предоставление субъекту персональных данных сведений, предусмотренных частью 3 настоящей статьи, нарушает права и законные интересы третьих лиц.

7. Права и обязанности работников оператора

7.1.Работники Оператора, имеющие доступ к персональным данным обучающегося, обязаны:
- не сообщать персональные данные обучающегося третьей стороне без письменного согласия одного из родителей (законного представителя), самого учащегося 18 лет, кроме случаев, когда в соответствии с федеральными законами такого согласия не требуется;
- использовать персональные данные обучающегося, полученные только от него лично или с письменного согласия одного из родителей (законного представителя);
- обеспечить защиту персональных данных обучающегося от их неправомерного использования или утраты в порядке, установленном законодательством Российской Федерации;
- ознакомить родителей, самого учащегося 18 лет, или законного представителя с настоящим Положением и их правами и обязанностями в области защиты персональных данных, под роспись;
- соблюдать требование конфиденциальности, персональных данных обучающегося;
- исключать или исправлять по письменному требованию одного из родителей (законного представителя) самого обучающегося 18 лет его недостоверные или неполные персональные данные, а также данные, обработанные с нарушением требований законодательства;
- ограничивать персональные данные обучающегося при передаче уполномоченным работникам правоохранительных органов или работникам Департамента образования только той информацией, которая необходима для выполнения указанными лицами их функцией;
- запрашивать информацию о состоянии здоровья обучающегося только у родителей (законных представителей) самого учащегося в возрасте 18 лет;
- обеспечить обучающемуся или одному из его родителей (законному представителю) свободный доступ к его персональным данным, включая право на получение копий любой записи, содержащей его персональные данные;
7.2. Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.

7.3. В случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя.
7.4. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных
7.5. Лица, имеющие доступ к персональным данным обучающегося, не в праве:
- получать и обрабатывать персональные данные обучающегося о его религиозных и иных убеждениях, семейной и личной жизни;
- предоставлять персональные данные обучающихся в коммерческих целях.

8. Доступ к персональным данным
8.1.Персональные данные добровольно передаются работником непосредственно специалисту по кадрам, исключительно для обработки и использования в работе.
8.2.Внешний доступ.
К числу внешних потребителей персональных данных работников относятся:
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.
8.3. Внутренний доступ.
К разряду потребителей персональных данных относятся работники, которым эти данные необходимы для выполнения должностных обязанностей:
- руководитель учреждения;
- работники бухгалтерии;
- руководители структурных подразделений.
8.4.В отделе кадров хранятся личные карточки работников, работающих в настоящее время. Для этого используются специально оборудованные шкафы или сейфы, которые запираются. Личные карточки располагаются в алфавитном порядке. После увольнения документы по личному составу передаются на хранение в архив.

9. Передача персональных данных работника
9.1. При передаче персональных данных работника Работодатель должен соблюдать следующие требования:
-не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;
-не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

-предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.
Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности).
Данное положение не распространяется на обмен персональными данными работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами;
-осуществлять передачу персональных данных работника в соответствии с настоящим Положением, с которым работник должен быть ознакомлен под роспись;
-разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
-не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
-передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

10. Защита персональных данных

10.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.
10.2.Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.
10.3.Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации.
10.4 «Внутренняя защита».
10.4.1. Для защиты персональных данных работников необходимо соблюдать ряд мер:
- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест, при котором исключается бесконтрольное использование защищаемой информации;
- знание работниками требований нормативно
- методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- проведение разъяснительной работы с работниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места.
Личные дела могут выдаваться на рабочие места только директору и в исключительных случаях, по письменному разрешению директора руководителю структурного

подразделения; - персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа.
10.5. «Внешняя защита».
10.5.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.
10.5.2.Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Работодателя, посетители, сотрудники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов Работодателя.
10.6. Для защиты персональных данных работников необходимо соблюдать ряд мер: - порядок приема, учета и контроля деятельности посетителей; - пропускной режим; - порядок охраны территории, зданий, помещений; - требования к защите информации при интервьюировании и собеседованиях.

11.Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работников

11.1.Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
11.2.Каждый работник, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.
11.3.Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Приложение 1

Письменное согласие работника на получение
его персональных данных у третьей стороны

Я, _____ в соответствии со ст. 86 ТК РФ _____ на получение моих персональных данных, (согласен, не согласен) а именно: _____
у_____
(Ф.И.О. физического лица или наименование организации, у которых получается

информация) О целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение предупрежден.

«_____» _____ 20___ г. _____(подпись) (Ф.И.О. работника)

Примечание:
1. Вместо паспорта могут указываться данные иного основного документа, удостоверяющего личность работника.
2. Письменное согласие работника заполняется и подписывается им собственноручно, в присутствии сотрудника отдела кадров.
3. Перечень персональных данных уточняется исходя из целей получения согласия.

Приложение 2

Журнал учета передачи персональных данных

п/ п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Дата передачи персональных данных	Подпись запрашивающего лица	Подпись ответственного сотрудника (оператора)

Приложение 3

Перечень должностей работников, имеющих доступ к персональным данным работников, которым они необходимы в связи с исполнением трудовых обязанностей
- руководители;
- заместители руководителей (в рамках своих должностных обязанностей);
- инспектор по кадрам;
- специалисты (в рамках своих должностных обязанностей);
- педагоги (только к персональным данным обучающегося);
- бухгалтер;
- программист;
- юрист.

Приложение 4

Руководителю
От_____
(фамилия, имя, отчество)
зарегистрированного по адресу: _____
(адрес регистрации указывается с почтовым индексом)
паспорт серия _____
_____ выдан
_____
(дата выдачи и наименование органа, выдавшего документ)

СОГЛАСИЕ
на обработку персональных данных

я,_____
(фамилия, имя, отчество полностью)
в соответствии со статьей 9 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" даю согласие организации на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно совершение действий, предусмотренных пунктом 3 части первой статьи 3 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных", со сведениями о фактах, событиях и обстоятельствах моей жизни, представленных в организации.
Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

_____ _____
(подпись) (расшифровка подписи)
_____ (дата)

Приложение 5

Руководителю
от_____
(ФИО, должность работника)
_____
(год рождения)
проживающий по адресу:
_____
паспорт: _____выдан:_____

Письменное согласие работника на передачу персональных данных третьей стороне

Я, _____ в соответствии со ст. 88 Трудового кодекса РФ _____ на передачу моих персональных данных, (согласен/не согласен) а именно:
1. фамилия, имя, отчество;
2. паспортные данные;
3. год, месяц, дата и место рождения;
4. адрес;
5. семейное, социальное, имущественное положение;
6. образование;
7. профессия;
8. сведения о трудовом и общем стаже;
9. доходы, полученные мной в данном учреждении;
10. сведения о воинском учете;
11. телефон

_____ для обработки в целях
_____
следующими лицам_____
(указываются Ф.И.О. физического лица или наименование организации, которым сообщаются данные)
_____
Согласие на передачу персональных данных третьей стороне действительно в течение всего срока действия трудового договора.
Подтверждаю, что ознакомлен с Положением об обработке и защите персональных данных работников, права и обязанности в области защиты персональных данных мне разъяснены, а также право работодателя обрабатывать (в том числе и передавать) часть моих персональных данных без моего согласия, в соответствии с законодательством РФ.
Подтверждаю, что отзыв согласия производится в письменном виде в соответствии с действующим законодательством. Всю ответственность за неблагоприятные последствия отзыва согласия беру на себя.
«_____» _____ 20___ г. _____
(подпись) (Ф.И.О. работника)
Примечание:
1. Вместо паспорта могут указываться данные иного основного документа, удостоверяющего личность работника.
2. Письменное согласие работника заполняется и подписывается им собственноручно, в присутствии сотрудника отдела кадров.
3. Перечень персональных данных не является исчерпывающим и уточняется исходя из целей получения согласия.

Приложение 6

Акт приема-передачи документов
(иных материальных носителей), содержащих персональные данные работника

Во исполнение договора на оказание услуг №_____ от_____ 20__ г., заключенного между организацией и,_____ (наименование организации, принимающей документы иные материальные носители), содержащие персональные данные работника) Учреждение, в лице
_____ (Ф.И.О., должность работника, осуществляющего передачу персональных данных работника) передает, а
_____
(наименование организации, принимающей документы (иные материальные носители), содержащие персональные данные работника) в лице

_____
(Ф.И.О., должность представителя организации, принимающей документы (иные материальные носители), содержащие персональные данные работника) получает документы (Ф.И.О., должность представителя организации, принимающей документы (иные материальные носители), содержащие персональные данные работника) (иные материальные носители), содержащие персональные данные работника на срок_ и в целях: (указать цель использования)
Перечень документов (иных материальных носителей), содержащих персональные данные работника:
№ Кол-во Всего
Полученные персональные данные работника могут быть использованы лишь в целях, для которых они сообщены. Незаконное использование предоставленных персональных данных путем их разглашения, уничтожения и другими способами, установленными федеральными законами, может повлечь соответствующую гражданско-правовую, материальную, дисциплинарную, административно-правовую и уголовную ответственность.
Передал
_____
(ФИО., должность работника Учреждения, осуществляющего передачу персональных данных работника)
Принял
_____
(Ф.И.О., должность, представителя организации - приемщика документов (иных материальных носителей), содержащих персональные данные работника)

СОГЛАСОВАНО:
Председатель первичной профсоюзной организации
МБДОУ «Детский сад № 49 «Радуга»
_____М.В.Хмельницкая

УТВЕРЖДЕНО:
Заведующий
МБДОУ «Детский сад № 49«Радуга»
_____О.Н.Заречнева
приказ № 195-од от 25.12.2020 года.

.

ПОЛОЖЕНИЕ
о защите персональных данных, обрабатываемых в информационных системах МБДОУ «Детский сад № 49 «Радуга»

1. **Общие положения**

Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации. Разработано на основе и во исполнение статей 23, 24 Конституции Российской Федерации, главы 14 Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». В целях соблюдения законодательства Российской Федерации в части обеспечения 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 в информационных системах персональных данных МБДОУ «Детский сад № 49 «Радуга».

Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом Российской Федерации от 27 июля 2006 г.
№ 152-ФЗ «О персональных данных», ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология – Практические правила управления информационной безопасностью», ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», «Базовая Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» Утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г., «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г., Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 г. Москва «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», Сборник руководящих документов по защите информации от несанкционированного доступа, Утвержден Председателем Гостехкомиссии России, 1997 г., Письмо Федерального агентства по образованию от 29.07.2009 № 17-110 «Об обеспечении защиты персональных данных», Письмо Федерального агентства по образованию от 03.09.2009 № 17-02-09/185 «О представлении уведомлений об обработке персональных данных», Письмо Федерального агентства по образованию от 22.10.2009 № 17-187 «Об обеспечении защиты персональных данных».

Список использованных понятий, терминов и сокращений

В настоящем Положении и для его целей используются следующие основные понятия, термины и сокращения:

ПДн - персональные данные.

ИСПДн - информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Оператор - администрация (орган администрации) Города Томска в лице своих Представителей, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных.

Цель обработки ПДн Субъекта - конкретный конечный результат действий, совершенных с персональными данными Субъекта, вытекающий из требований законодательства и направленный, в том числе на создание необходимых правовых условий для достижения оптимального согласования интересов сторон трудовых отношений.

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

Блокирование ПДн - временное прекращение сбора, систематизации, накопления, использования, распространения ПДн, в том числе их передачи.

Обезличивание ПДн - действия, в результате которых невозможно определить принадлежность ПДн конкретному Субъекту персональных данных.

Представитель(и) оператора - лицо(а), которые в соответствии с договором, должностными обязанностями или внутренними документами администрации (органа администрации), уполномочены на доступ или обработку ПДн Субъектов.

Субъект ПДн - физическое лицо, персональные данные которого обрабатываются в ИСПДн.

Обработка ПДн - действия (операции) с персональными данными, включая сбор, просмотр, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Использование ПДн - действия (операции) с персональными данными, совершаемые Оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении Субъекта или других лиц либо иным образом затрагивающих права и свободы Субъекта или других лиц.

Уничтожение ПДн - действия, в результате которых невозможно восстановить содержание ПДн в ИСПДн или в результате которых уничтожаются материальные носители ПДн.

Распространение ПДн - действия, направленные на передачу ПДн определенному кругу лиц (передача ПДн) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Конфиденциальность ПДн - обязательное для соблюдения Оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия Субъекта или наличия иного законного основания.

Общедоступные ПДн - ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия Субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2. Классификация информационных систем персональных данных и определение актуальных угроз их безопасности

Перечень типовых ИСПДн определен приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

Классификация ИСПДн осуществляется в зависимости от категории персональных данных (ПДн), не содержащих сведения, относящиеся к государственной тайне:
Категория 1 – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
Категория 2 – ПДн, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1;
Категория 3 – ПДн, позволяющие идентифицировать субъекта персональных данных;
Категория 4 – обезличенные и/или общедоступные персональные данные.

3. Понятие и состав ПДн

Для целей настоящего Положения ПДн признается любая информация, относящаяся к определенному или определяемому на основании такой информации Субъекту, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, фотография, индивидуальный номер налогоплательщика, номер страхового свидетельства обязательного пенсионного страхования, данные квалификационного аттестата, другая информация.

Субъектами ПДн в ИСПДн являются:
работники организаций; граждане, исполняющие обязанности по техническому обеспечению деятельности организаций; граждане, выполняющие работы и оказывающие услуги в организациях по гражданско-правовым договорам; граждане, обратившиеся в организации в соответствии с Федеральным законом от 02.05.2006 №59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
иные граждане в случаях, предусмотренных действующим законодательством.
Документами, содержащими ПДн, являются:

а) паспорт или иной документ, удостоверяющий личность;

б) трудовая книжка;

в) страховое свидетельство государственного пенсионного страхования;

г) свидетельство о постановке на учёт в налоговый орган и присвоения ИНН;

д) документы воинского учёта;

е) документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;

ж) карточка Т-2;

з) автобиография;

и) квалификационный аттестат;

к) другие документы, содержащие данные, идентифицирующие Субъекта.
Документы, содержащие ПДн, создаются путём:
а) копирования подлинников (например, копии документов об образовании, свидетельство ИНН, пенсионных свидетельств Субъектов);
б) заполнения анкетных данных (на бумажных и электронных носителях);
в) предоставления подлинников документов (трудовых книжек, личные листки по учёту кадров, автобиографии Субъектов);
г) внесения информации о Субъекте ПДн в ИСПДн (на бумажные и электронные носители);
д) иными способами.

4. Порядок обработки персональных данных субъектов

Обработка ПДн Субъектов осуществляется в следующих целях:
соблюдения законов и иных нормативных правовых актов, в том числе в целях реализации прав Субъектов ПДн;
содействия Субъектам ПДн в трудоустройстве, обучении и повышении в должности;
обеспечения личной безопасности Субъектов ПДн;
обеспечения сохранности имущества Субъектов ПДн;
в иных целях, предусмотренных действующим законодательством.

Обработка ПДн Субъектов должна осуществляться на основе принципов:
законности целей и способов обработки ПДн и добросовестности;
соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям Оператора;
достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн; недопустимости объединения созданных для несовместимых между собой целей баз данных ИС ПДн;
соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн.

При определении объема и содержания обрабатываемых ПДн Субъекта, Оператор ПДн должен руководствоваться Конституцией Российской Федерации и федеральными законами.

Оператор при обработке ПДн Субъекта обязан соблюдать следующие требования: Все ПДн Субъекта следует получать у него самого. В случае возникновения необходимости получения ПДн Субъекта у третьей стороны Оператор обязан известить об этом Субъекта ПДн, получить его письменное согласие и сообщить Субъекту о целях, предполагаемых источниках и способах получения ПДн, а также о характере подлежащих получению ПДн и последствиях отказа Субъекта дать письменное согласие на их получение.

Обеспечения конфиденциальности ПДн не требуется:
в случае обезличивания ПДн Субъекта;
в отношении общедоступных ПДн Субъектов, которые создаются в целях информационного обеспечения деятельности администрации (в том числе справочники, адресные книги). В общедоступные источники ПДн Субъектов с письменного согласия Субъекта могут включаться его фамилия, имя, отчество, год и место рождения, адрес и иные ПДн, предоставленные Субъектом.

Сведения о Субъекте должны быть в любое время исключены из общедоступных источников ПДн по требованию Субъекта, либо по решению суда или иных уполномоченных государственных органов.

За исключением случаев, предусмотренных федеральными законами, Оператор не имеет права обрабатывать следующие ПДн Субъекта:
о политических, религиозных философских и иных убеждениях и частной жизни;
о расовой и национальной принадлежности;
о членстве в общественных объединениях или профсоюзной деятельности;
о состоянии здоровья;
об иных ПДн, предусмотренных федеральными законами.

Оператор не вправе запрашивать информацию о состоянии здоровья Субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения Работником трудовой функции.

Оператор осуществляет обработку ПДн Субъекта как в автоматизированной, так и в неавтоматизированной форме. Особенности способов обработки ПДн (автоматизированная/ неавтоматизированная) и защиты ПДн может быть установлена муниципальными правовыми актами Оператора в соответствии с требованиями, предусмотренными действующим законодательством.

При передаче ПДн Оператор не вправе:
сообщать ПДн Субъекта третьей стороне без письменного согласия Субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Субъекта, а также в других случаях, предусмотренных федеральными законами.
сообщать ПДн Субъекта в коммерческих целях без его письменного согласия.

При передаче ПДн Оператор обязан:
предупредить лиц, получающих ПДн Субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие ПДн Субъекта,

обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными Субъектов в порядке, установленном федеральными законами;
за счет своих средств обеспечить защиту ПДн Субъекта от неправомерного их использования или утраты в порядке, установленном федеральным законом;
ознакомить Субъектов, являющихся работниками Оператора, и их представителей под роспись с документами администрации, устанавливающими порядок обработки ПДн Субъектов, а также об их правах и обязанностях в этой области;
разъяснить Субъекту, являющемуся работником (лицом, принимаемым на работу) юридические последствия отказа предоставить ПДн (например - невозможность осуществления работодателем своих функций, указать нормы законодательства, требующие предоставления ПДн);
разрешать доступ к персональным данным Субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те ПДн Субъекта, которые необходимы для выполнения конкретных функций;
выполнять иные обязанности. предусмотренные федеральными законами и настоящим Положением.

ПДн Субъекта могут быть переданы представителям Субъектов в порядке, установленном Трудовым Кодексом Российской Федерации и иными федеральными законами, в том объеме, в каком это необходимо для выполнения указанными представителями их функций.

Предоставление сведений о ПДн Субъектов без соответствующего их согласия возможно только в случаях, предусмотренных федеральными законами. Трансграничная передача ПДн осуществляется в порядке, предусмотренном действующим законодательством Российской Федерации.

В случае достижения цели обработки ПДн Субъектов Оператор обязан незамедлительно прекратить обработку ПДн Субъекта и уничтожить соответствующие ПДн в срок, не превышающий трех рабочих дней с даты достижения цели обработки ПДн, если иное не предусмотрено федеральными законами и уведомить об этом Субъекта или его законного представителя.

Достижением цели обработки ПДн Субъекта, как правило, является истечение сроков хранения документов.

Порядок хранения ПДн Субъектов, являющихся работниками Оператора, устанавливается Оператором с соблюдением требований законодательства Российской Федерации.

Иные требования к обработке ПДн Субъекта определяются действующим трудовым законодательством и законодательством о защите персональных данных.

5. Разрешительные документы о допуске конкретных сотрудников к обработке персональных данных

Приказы или иные утвержденные руководством учреждения разрешительные документы должны включать списки сотрудников Оператора и временно привлекаемых лиц, допущенных к обработке укрупненных групп персональных данных. Работа с персональными данными лиц, не включенных в разрешительные документы, не допускается.

6. Приказ о возложении персональной ответственности за защиту персональных данных

В приказе рекомендуется привести список конкретных лиц, ответственных за защиту информационных систем и групп обрабатываемых в учреждении персональных данных.

7. Ответственность должностных лиц по обеспечению защиты персональных данных субъектов.

Руководители организаций несут ответственность обеспечение защиты ПДн Субъектов в соответствии с настоящим положением и иными руководящими нормативными

правовыми актами по защите ПДн; контроль за подчиненными в части выполнения требований нормативных правовых актов по вопросам защиты ПДн.

Ответственный за эксплуатацию объекта информатизации, содержащего ИСПДн, назначается приказом и отвечает за:

разработку и согласование проектов методической документации по защите ПДн Субъектов в ИСПДн;

качественное и своевременное выполнение должностными лицами установленных требований по защите ПДн Субъектов;

своевременную разработку и реализацию мер по защите ПДн Субъектов,

организацию и проведение контроля состояния защиты ПДн Субъектов в ИСПДн;

определение степени опасности технических каналов утечки информации, различных способов НСД к ПДн Субъектов, их разрушения (уничтожения) или искажения;

организацию проведения расследований по фактам нарушений в области защиты ПДн Субъектов и разработку предложений по устранению недостатков и предупреждению подобного рода нарушений;

анализ состояния работ по защите ПДн Субъектов и разработку предложений по совершенствованию системы защиты ПДн в ИСПДн;

организацию и проведение занятий с работниками по вопросам защиты ПДн Субъектов;

планирование и организацию защиты ПДн Субъектов в ИСПДн;

выполнение требований действующих нормативных и руководящих документов и защиты сведений, отнесенных к конфиденциальной информации, при проведении работ в ИСПДн.

определение необходимых мер по защите ПДн Субъектов, организацию их разработки и реализации;

обеспечение бесперебойного функционирования программных и аппаратных средств в ИСПДн;

ознакомление работников, которые допускаются к обработке ПДн, с настоящим Положением;

ознакомление сотрудников, которые участвуют в обработке ПДн, с должностными инструкциями по работе и обеспечению режима информационной безопасности в ИСПДн;

соблюдение пользователями ИСПДн установленных правил и параметров печати, регистрации и учета документов, а также регистрации и учета бумажных и машинных носителей информации;

проведение анализа возможности решения определенных задач на ИСПДн и уточнение содержания необходимых для этого изменений в конфигурации аппаратных и программных средств;

взаимодействие с администратором безопасности ИСПДн по вопросам обеспечения правильного использования пользователями СЗИ от НСД и контроля доступа этих пользователей к работе в ИСПДн;

ведение и хранение документации на ИСПДн;

организацию технического обслуживания (ремонта, модернизации) ПЭВМ и других технических средств ИСПДн;

установку (развертывание, обновление версий) программных средств, необходимых для решения в ИСПДн конкретных задач;

удаление программных средств, необходимость в использовании которых отпала; установку (развертывание) новых ИСПДн или подключение дополнительных устройств (узлов, блоков), необходимых для решения конкретных задач (по согласованию с руководителями);

установку, подключение и настройку технических средств в ИСПДн в соответствии с документацией к ним и планами организации и оснащения ИСПДн по согласованию с руководителем структурного подразделения, к которому имеет отношение ИСПДн.;

контроль за обеспечением защиты ПДн Субъектов в ИСПДн;

своевременное обнаружение фактов несанкционированного доступа к ПДн Субъектов; проводит работы по разработке, внедрению, совершенствованию и эксплуатации системы защиты ПДн Субъектов в ИСПДн;

организацию (при необходимости) контрольных проверок ИСПДн;

установку и ввод в эксплуатацию средств защиты ПДн Субъектов в соответствии с эксплуатационной и технической документацией к ним; организацию в установленном порядке расследования причин и условий появления нарушений по вопросам технической защиты ПДн Субъектов, разработку предложений по устранению недостатков и предупреждению подобного рода нарушений;

проведение анализа возможности решения (а также совмещения) указанных задач в конкретных ИСПДн (с точки зрения обеспечения безопасности) и принятие решения об отнесении их к той или иной группе по степени защищенности; проведение необходимых дополнительных специальных мероприятий по обеспечению безопасности ПДн;

внедрение средств контроля эффективности противодействия попыткам НСД к информации и незаконного вмешательства в процесс функционирования ИСПДн.

8. Права, обязанности и ответственность субъекта персональных данных и Оператора при обработке персональных данных

– права субъекта персональных данных в целях обеспечения защиты своих персональных данных (в целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ «О персональных данных» за исключением случаев, предусмотренных данным Федеральным законом, имеет право на получение сведений об Операторе, о месте его нахождения, о наличии у Оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными; требовать от Оператора уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав; на получение при обращении или при получении запроса информации, касающейся обработки его персональных данных; на обжалование действий или бездействия Оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и/или компенсацию морального вреда в судебном порядке);

– обязанности Оператора при сборе персональных данных (Оператор обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или блокировать соответствующие персональные данные по предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет Оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы; в случае выявления неправомерных действий с персональными данными Оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении

допущенных нарушений или об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных или его законного представителя;

– в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Оператором и субъектом персональных данных. Об уничтожении персональных данных Оператор обязан уведомить субъекта персональных данных);

– права Оператора на передачу персональных данных третьим лицам (Оператор не вправе без письменного согласия субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации);

– ответственность Оператора за разглашение персональных данных (Оператор, а также должностные лица, виновные в нарушении требований настоящего Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Ответственность за соблюдение требований законодательства Российской Федерации при обработке и использовании персональных данных возлагается в приказе об утверждении Положения и иных приказах на руководителей структурных подразделений и конкретных должностных лиц Оператора, обрабатывающих персональные данные).

9. Доступ к персональным данным субъекта

Доступ к ПДн Субъекта ограничивается в соответствии с федеральными законами и настоящим Положением. Доступ к ПДн Субъектов имеют только работники, в соответствии с «Матрицей разграничения доступа к защищаемым ресурсам».

Разрешительная система допуска лиц (должностей), в обязанности которых входит обработка ПДн или которые по должности имеют доступ к персональным данным с правом просмотра, разрабатывается ответственным за эксплуатацию объекта информатизации, содержащего ИСПДн.

Представители Оператора имеют право получать только те ПДн Субъекта, которые необходимы для выполнения конкретных функций в соответствии с должностной инструкцией указанных лиц. Все остальные работники Оператора, являющиеся Субъектами ПДн, имеют право на полную информацию только о своих ПДн.

Внешний доступ (доступ лицами, не являющимися представителями Оператора и Субъектами ПДн): получение сведений о ПДн Субъектов третьей стороной разрешается только при наличии заявления с указанием конкретных ПДн, целей, для которых они будут использованы, способов обработки, иных сведений, установленных действующим законодательством, а также письменного согласия Субъекта, ПДн которого затребованы в порядке, предусмотренном Трудовым кодексом Российской Федерации и Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

10. Меры по защите персональных данных субъекта

Документы, содержащие ПДн Субъекта, должны передаваться между подразделениями в запечатанном конверте с пометкой «ПЕРСОНАЛЬНЫЕ ДАННЫЕ».

Оператор определяет перечень своих Представителей, имеющих право доступа и обработки информации о ПДн, и соответствующие уровни доступа к этой информации.

Оператор утверждает формы ведения учета выданных ПДн (если соответствующие формы не определены действующим законодательством) и уполномочивает своих Представителей на их ведение.

При автоматизированной обработке ПДн Оператор использует специальное программное обеспечение и аппаратные средства, соответствующее предусмотренным действующим законодательством требованиям.

Оператор в предусмотренном Трудовым кодексом Российской Федерации порядке проводит ознакомление Субъектов, являющихся работниками Оператора, с нормативными правовыми актами и в области защиты ПДн, в том числе в случае их изменения, разъясняет права, обязанности и ответственность Субъектов за нарушение норм в данной области.

Оператор устанавливает особый режим хранения для документов, содержащих ПДн Субъектов. ПДн Субъектов, содержащиеся на бумажных носителях, должны храниться в запираемом шкафу или в сейфе.

Ключи от кабинетов уполномоченных Представителей сдаются при выходе из здания под охрану.

Доступ к персональным данным Субъекта, содержащимся в ИСПДн, ограничивается определенными Оператором сотрудниками.

Сроки хранения документов устанавливаются Оператором соответствующим муниципальным правовым актом в соответствии с требованиями действующего законодательства.

11. Ответственность за разглашение конфиденциальной информации, содержащей персональные данные субъектов

Лица, виновные в нарушении действующего законодательства, муниципальных правовых актов, регулирующих обработку и защиту ПДн Субъекта, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

Порядок организации учета, хранения, выдачи и уничтожения съемных носителей, содержащих персональные данные

Настоящий Порядок организации учета, хранения, выдачи и уничтожения съемных носителей, содержащих персональные данные, в целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, разработан с учетом Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", в соответствии с Федеральным законом 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", методическими рекомендациями ФСТЭК России от 15.02.2008, утвержденные приказом ФСТЭК России от 05.02.2010 № 58 "Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных", и устанавливает порядок использования съемных носителей информации, используемых в информационных системах персональных данных (далее – ИСПДн) в организациях.

Учет, хранение, выдачу и уничтожение съемных носителей персональных данных осуществляют ответственные лица за эксплуатацию ИСПДн. При увольнении сотрудника, ответственного за учет, хранение и выдачу съемных носителей персональных данных, составляется акт приема–передачи этих документов, который утверждается руководителем организации или его заместителем.

Организация учета съемных носителей персональных данных.

Все находящиеся на хранении и в обращении съемные носители персональных данных подлежат учёту. Учет всех видов и типов носителей производится в журнале учета съемных носителей, содержащих персональные данные.

Каждый носитель должен иметь этикетку, на которой указывается его уникальный учетный номер. На несъемной части упаковки носителя ПДн указывается:

– учетный номер;
– отметка "Персональные данные";
– дата регистрации (день, месяц, год);
– ФИО, должность, подпись сотрудника выполнившего учет.

12. Организация выдачи съемных носителей персональных данных

Пользователи ИСПДн получают учтенный съемный носитель у ответственного лица за организацию обработки персональных данных. При получении делаются соответствующие записи в журнале учета съемных носителей, содержащих персональные данные.

13. Организация хранения съемных носителей персональных данных

Хранение носителей осуществляется в условиях, исключающих несанкционированное копирование, изменение или уничтожение информации ограниченного доступа, а также хищение носителей. Носители должны храниться в служебных помещениях, в металлическом шкафу (сейфе).

Запрещается хранить съемные носители персональных данных вместе с носителями открытой информации, на рабочих столах, оставлять их без присмотра или передавать на хранение другим лицам, выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, а также использовать носители персональных данных в личных целях.

В случае утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений, ставится в известность ответственное лицо за организацию обработки персональных данных в Управлении. Соответствующие отметки вносятся в журнал учета съемных носителей, содержащих персональные данные.

Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется комиссией. По результатам уничтожения носителей составляется акт уничтожения съемных носителей персональных данных).

Ответственность за выполнение правил эксплуатации съемных носителей персональных данных при выполнении непосредственных работ с носителями несет пользователь ИСПДн.

Контроль выполнения пользователями установленных правил эксплуатации съемных носителей персональных данных, осуществляет ответственное лицо за организацию обработки персональных данных.

Специалисты, нарушившие требования настоящего порядка, несут ответственность в соответствии с действующим законодательством.

14. Инструкция пользователя при обработке персональных данных на объектах вычислительной техники

Общие положения:

– предмет Инструкции (основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) учреждения);

– общие требования к пользователю (пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ и несет персональную ответственность за соблюдение требований руководящих документов по защите информации).

Обязанности пользователя:

– выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные в настоящей Инструкции;

– при работе с персональными данными не допускать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, или располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра, отображаемой на нем информации посторонними лицами;

– соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с персональными данными при ее обработке;
– после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ПЭВМ;
– оповещать обслуживающий ПЭВМ персонал, а также непосредственного начальника о всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
– не допускать «загрязнение» ПЭВМ посторонними программными средствами;
– знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий;
– знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;
– помнить личные пароли, персональные идентификаторы не оставлять без присмотра и хранить в запирающемся ящике стола или сейфе;
– знать штатные режимы работы программного обеспечения, знать пути проникновения и распространения компьютерных вирусов;
– при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов;
– при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции;
– в случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:
– приостановить работу;
– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного начальника, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
– оценить необходимость дальнейшего использования файлов, зараженных вирусом;
– провести лечение или уничтожение зараженных файлов (при необходимости, для выполнения требований данного пункта следует привлечь администратора системы).
Запрещаемые действия:
– записывать и хранить персональные данные на неучтенных установленным порядком машинных носителях информации;
– удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
– самостоятельно подключать к ПЭВМ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ПЭВМ;
– самостоятельно устанавливать и/или запускать (выполнять) на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
– осуществлять обработку персональных данных в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска, а также при несоблюдении требований по эксплуатации ПЭВМ;
– сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
– отключать (блокировать) средства защиты информации;
– производить какие-либо изменения в подключении и размещении технических средств;
– производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;
– оставлять бесконтрольно ПЭВМ с загруженными персональными данными, с установленными маркированными носителями, электронными ключами, а также распечатываемыми бумажными документами с персональными данными.
Права пользователя ПЭВМ:

– обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;
– обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и
прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.
Ответственность пользователей ПЭВМ за:
– надлежащее выполнение требований настоящей инструкции;
– соблюдение требований нормативных документов и инструкций, определяющих порядок организации работ по защите информации и использования информационных ресурсов;
– сохранность и работоспособное состояние средств вычислительной техники ПЭВМ;
– сохранность персональных данных.
Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

15. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

Общие положения, в том числе:
– предмет Инструкции (обязательные для всех структурных подразделений учреждения требования по обеспечению конфиденциальности документов, содержащих персональные данные);
– определение персональных данных (персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация);
– когда обеспечение конфиденциальности персональных данных не требуется (в случае обезличивания персональных данных или в отношении общедоступных персональных данных. В общедоступные источники персональных данных (в том числе справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных);
– необходимость согласия субъекта персональных данных или наличие иного законного основания на их обработку (конфиденциальность персональных данных предусматривает обязательное согласие субъекта персональных данных или наличие иного законного основания на их обработку).
Согласие субъекта персональных данных не требуется на обработку:
– данных в целях исполнения обращения, запроса субъекта персональных данных, трудового или иного договора с ним;
– адресных данных, необходимых для доставки почтовых отправлений организациями почтовой связи;
– данных, включающих в себя только фамилии, имена и отчества;
– данных в целях однократного пропуска на территорию, или в иных аналогичных целях;
– персональных данных, обрабатываемых без использования средств автоматизации;
– порядок ведения перечней персональных данных (в структурных подразделениях учреждения формируются и ведутся перечни конфиденциальных данных с указанием регламентирующих документов, мест хранения и ответственных за хранение и обработку данных. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень,
запрещается);
– нормативные документы, определяющие основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных и

использования средств автоматизации (Основные требования и мероприятия по обеспечению безопасности при обработке и хранении персональных данных установлены постановлениями Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации». Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее);

– общие правила хранения и передачи персональных данных (запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении. Все сотрудники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных).

Сотрудникам, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа в соответствии с резолюцией, файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

Передача персональных данных допускается только в случаях, установленных Федеральными законами Российской Федерации «О персональных данных», «О порядке рассмотрения обращений граждан Российской Федерации», действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

Ответственность за защиту обрабатываемых персональных данных (например, сотрудники подразделений учреждения, сотрудники организаций-
Операторов или лица, осуществляющие такую обработку по договору с Оператором, а также иные лица, осуществляющие обработку или хранение конфиденциальных данных в «учреждении», несут ответственность за обеспечение их информационной безопасности. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную или уголовную ответственность в соответствии с законодательством и ведомственными нормативными актами).

Порядок ознакомления с Инструкцией (сотрудники подразделений учреждения и лица, выполняющие работы по договорам и контрактам, имеющие отношение к работе с персональными данными, должны быть в обязательном порядке ознакомлены под расписку с настоящей Инструкцией).

Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемой с использованием средств автоматизации, в том числе, правила доступа, хранения и пересылки персональных данных (например, безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии).

Допуск лиц к обработке персональных данных в информационной системе осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

Размещение информационных систем, специальное оборудование и организация работы с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

Компьютеры и/или электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе по Интернету, запрещается.

Общие требования по защите персональных данных в автоматизированных системах (например, технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия).

При обработке персональных данных в информационной системе пользователями должно быть обеспечено:

– использование предназначенных для этого раздела (каталога) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

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

– постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– недопущение несанкционированного выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

При обработке персональных данных в информационной системе разработчиками и администраторами систем должны обеспечиваться:

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет лиц, допущенных к работе с персональными данными в информационной системе, прав и паролей доступа;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

– контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– описание системы защиты персональных данных.

Специфические требования по защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации, в том числе:

– организация учета носителей персональных данных – все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

Учет и выдачу съемных носителей персональных данных осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Сотрудники учреждения получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

Правила использования съемных носителей персональных данных:

– запрещается хранить съемные носители с персональными данными вместе с носителями открытой информации на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– запрещается выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

Порядок действий при утрате или уничтожении съемных носителей персональных данных (например, о фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт.

Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных).

Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт.

При осуществлении обработки персональных данных с использованием средств автоматизации для каждой информационной системы персональных данных должен быть назначен администратор, а для системы высоких классов – также администратор системы безопасности. Инструкции для этого должностного лица составляются отдельно. Для технического обслуживания оборудования должен быть предусмотрен соответствующий обслуживающий персонал.

Приложение 1

Типовая форма
журнала учета съемных носителей персональных данных

Начат "___" _____ 20__ года на _____ листах
Окончен "___" _____ 20__ года

_____ _____
Должность и Ф.И.О., ответственного за хранение Подпись

№ п/п	Регистрационный номер/дата	Тип/ёмкость машинного носителя персональных данных	Номер экземпляра/ количество экземпляров	Место установки (использования)/дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации

									(подпись, дата)

Приложение 2

АКТ
уничтожения съемных носителей персональных данных

Комиссия в составе:

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему использованию (хранению):

№ п/п	Дата регистрации	Учетный номер съемного носителя	Примечание

Всего съемных носителей_____
(цифрами и прописью)

На съемных носителях уничтожены персональные данные путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены
путем _____
(разрезания, демонтажа, сжигания, крошения и т.п.)
Председатель комиссии_____
Подпись
Члены комиссии _____