Муниципальное автоновное дошкольное образовательное учреждение
«Центр развития ребенка – детский сад № 116» г. Сыктывкара
(МАДОУ «ЦРР – д/сад № 116» г. Сыктывкара)

УТВЕРЖДЕНО
приказом директора
МАДОУ «ЦРР – д/сад № 116» г. Сыктывкара
от «15»04 20 19 г. № 131

ПОЛОЖЕНИЕ

об обработке и защите персональных данных

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ

АРМ	– автоматизированное рабочее место;
ИТ	– информационные технологии;
Комиссия	– постоянно действующая комиссия по защите персональных данных;
ЛНА	– локальные нормативные акты;
МНИ	– машинные носители информации;
НСД	– несанкционированный доступ;
ПДн	– персональные данные;
СЗИ	– средство защиты информации;
Учреждение	– МАДОУ «ЦРР – д/сад № 116» г. Сыктывкара.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение

1.1.1. Положение об обработке и защите ПДн определяет особенности защиты и обработки ПДн в Учреждении, осуществляемой с использованием средств вычислительной техники и без использования таких средств.

1.1.2. Настоящее Положение определяет состав основных организационных и технических мер по обеспечению безопасности ПДн при их обработке в Учреждении.

1.1.3. Настоящее Положение разработано в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О ПДн».

1.2. Цели

1.2.1. Настоящее Положение принято в следующих целях:

– формализация условий и порядка обработки и защиты ПДн в Учреждении;

– обесчение защиты прав и свобод человека и гражданина при обработке его ПДн в Учреждении, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.3. Область применения

1.3.1. Действие Положения распространяется на все структурные подразделения Учреждения, осуществляющие обработку ПДн и на всех субъектов ПДн, чьи ПДн обрабатываются в Учреждении.

1.3.2. Настоящее Положение обязаны знать и использовать в работе лица, допущенные к обработке ПДн в Учреждении с использованием средств вычислительной техники и без использования таких средств.

1.3.3. Все лица, указанные в п.1.3.2 настоящего Положения, в обязательном порядке должны быть ознакомлены с ним под личную подпись.

1.3.4. Методическое руководство и контроль над соблюдением требований настоящего Положения, а также требований других ЛНА Учреждения, регламентирующих обработку и защиту ПДн в Учреждении, возлагается на Комиссию.

1.4. Вступление в силу

1.4.1. Настоящее Положение вступает в силу с момента его утверждения директором Учреждения и действует бессрочно до его замены или отмены.

1.5. Пересмотр

1.5.1. Настоящее Положение подлежит пересмотру в случаях:

– изменения законодательства РФ о ПДн;

– изменения условий и порядка обработки ПДн в Учреждении.

1.5.2. Все изменения в настоящее Положение вносятся приказом директора.

2. ПОНЯТИЕ И СОСТАВ ПДН

2.1. Понятие ПДн

2.1.1. ПДн - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

2.2. Состав ПДн

2.2.1. ПДн составляют:

– сведения о фактах, событиях и обстоятельствах частной жизни субъекта, позволяющие идентифицировать его, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

– служебные сведения, а также иные сведения, связанные с профессиональной деятельностью работников, в том числе сведения о поощрениях и о дисциплинарных взысканиях;

– сведения о расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн;

– сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Учреждением для установления личности субъекта ПДн.

2.2.2. Документами, содержащие ПДн являются:

– паспорт или иной документ, удостоверяющий личность;

– трудовая книжка;

– страховое свидетельство государственного пенсионного страхования;

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

– документы воинского учёта;

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

– карточка Т-2;

– личный листок по учёту кадров;

– документы, содержащие сведения о заработной плате, доплатах и надбавках;

– приказы о приеме на работу, об увольнении, о переводе лица на другую должность;

– медицинская и санитарная книжки;

– другие документы, содержащие сведения, указанные в пункте 2.2.1.

2.2.3. Состав обрабатываемых в Учреждении ПДн с указанием сроков хранения содержащих их документов определяется Перечнем обрабатываемых ПДн.

2.2.4. Субъектами ПДн в Учреждении являются:

– работники (в т.ч. уволенные) Учреждения;

– близкие родственники работников Учреждения;

– воспитанники;

– законные представители воспитанников;

– близкие родственники законных представителей воспитанников;

– соискатели.

2.2.5. Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические ПДн) в Учреждении не обрабатываются.

2.2.6. Учреждение обеспечивает конфиденциальность обрабатываемых ПДн, за исключением ПДн, которые в установленных федеральными законами случаях могут быть опубликованы в средствах массовой информации или иных общедоступных источниках информации, и не допускает их распространения без согласия субъекта ПДн, либо наличия иного законного основания. Документы, содержащие ПДн являются конфиденциальными. Гриф конфиденциальности на таких документах не проставляется.

3. ОБРАБОТКА ПДН

3.1. Условия

3.1.1. Субъект ПДн является собственником своих ПДн и самостоятельно принимает решение об их предоставлении Учреждению. В случае недееспособности либо несовершеннолетия субъекта ПДн решение о предоставлении его ПДн Учреждению принимает его законный представитель.

3.1.2. Обработка ПДн Учреждением ограничивается достижением целей обработки ПДн. Не допускается обработка ПДн, несовместимая с целями их сбора.

3.1.3. Обработка ПДн Учреждением осуществляется после:

– получения согласия субъекта ПДн, за исключением случаев, предусмотренных законодательством РФ;

– направления уведомления об обработке ПДн (о намерении осуществлять обработку ПДн) в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Республике Коми;

– принятия необходимых мер по обеспечению безопасности ПДн.

3.1.4. Все ПДн, полученные в виде незаверенных копий, заполненных типовых форм и бланков или со слов субъекта ПДн, проверяются работником Учреждения, осуществляющим их сбор, на соответствие оригиналам документов, принадлежащих данному субъекту ПДн.

3.1.5. Обработка ПДн допускается в следующих случаях:

– с согласия субъекта ПДн;

– обработка ПДн необходима для достижения целей, предусмотренных международным договором РФ или законом, для осуществления и выполнения, возложенных законодательством РФ на Учреждение функций, полномочий и обязанностей;

– обработка ПДн необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», для обеспечения предоставления такой услуги, для регистрации субъекта на едином портале государственных и муниципальных услуг;

– обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем;

– обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

– обработка ПДн необходима для осуществления прав и законных интересов Учреждения или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

– в статистических или иных исследовательских целях, за исключением целей, связанных с политической агитацией, продвижением товаров, работ и услуг на рынке;

– к ПДн предоставлен доступ неограниченному кругу лиц субъектом ПДн либо по его просьбе;

– ПДн подлежат опубликованию или обязательному раскрытию в соответствии с законодательством РФ.

3.1.6. Должностное лицо Учреждения, ответственное за кадровое обеспечение, обязано проводить дополнительные мероприятия, направленные на подтверждение факта направления резюме самим соискателем, в случае получения указанного резюме по каналам электронной почты или факсимильной связи. К таким мероприятиям относится приглашение соискателя на личную встречу с уполномоченными работниками Учреждения, обратная связь посредством электронной почты и т.д.

3.1.7. Работники Учреждения, осуществляющие сбор ПДн, разъясняют субъектам ПДн юридические последствия их отказа в предоставлении своих ПДн, если предоставление ПДн является обязательным в соответствии с законодательством РФ (трудовым законодательством, законодательством о медицинском, пенсионном и социальном страховании и др.).

3.1.8. Копировать и делать выписки из документов, содержащих ПДн, разрешается исключительно в служебных целях с письменного разрешения руководителя структурного подразделения.

3.1.9. При принятии решений, затрагивающих интересы работника Учреждения, работодатель не имеет права основываться на ПДн работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель должен учитывать личные качества работника, его добросовестный и эффективный труд.

3.2. Особенности автоматизированной обработки

3.2.1. Обработка ПДн с использованием средств вычислительной техники осуществляется в ИСПДн Учреждения.

3.2.2. Состав и характеристики ИСПДн Учреждения определяются Перечнем ИСПДн.

3.2.3. Обмен ПДн при их обработке в ИСПДн Учреждения осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения программных и технических средств. Не допускается передача ПДн по открытым (незащищенным) каналам связи, таким как телефон, факс и электронная почта.

3.2.4. МНИ, предназначенные для обработки ПДн, подлежат обязательной регистрации и учету в Журнале учета машинных носителей информации.

3.2.5. Права и обязанности работников Учреждения, допущенных к работе в ИСПДн Учреждения, определяются Инструкцией пользователя ИСПДн и другими ЛНА Учреждения.

3.3. Согласие субъекта ПДн

3.3.1. Обработка ПДн работников Учреждения не требует получения его согласия, при условии, что объем обрабатываемых Учреждением ПДн не превышает установленные законодательством РФ перечни, а также соответствует целям обработки, предусмотренным трудовым законодательством РФ.

3.3.2. Учреждение вправе осуществлять обработку ПДн своего работника без соответствующего согласия в случаях, предусмотренных коллективным договором, в том числе правилами внутреннего трудового распорядка, соглашением между работником и Учреждением, а также в случаях, предусмотренных ЛНА Учреждения, принятыми в порядке, установленном ст.372 Трудового кодекса РФ.

3.3.3. Обработка ПДн уволенного работника не требует получения соответствующего согласия при условии, что она осуществляется в рамках бухгалтерского и (или) налогового учета и соблюдаются сроки, предусмотренные законодательством РФ. После истечения сроков, предусмотренных законодательством РФ, личные дела работников Учреждения и иные документы передаются на архивное хранение, при этом на организацию архивного хранения, комплектование, учет и использование архивных документов, содержащих ПДн работников Учреждения, действие ФЗ «О ПДн» не распространяется.

3.3.4. Обработка ПДн соискателей на замещение вакантных должностей в рамках правоотношений, урегулированных Трудовым кодексом РФ, предполагает получение согласия соискателей на замещение вакантных должностей на обработку их ПДн на период принятия Учреждением решения о приеме либо отказе в приеме на работу. Исключение составляют случаи, когда от имени соискателя действует кадровое агентство, с которым соискатель заключил соответствующий договор, а также при самостоятельном размещении соискателем своего резюме в сети Интернет, доступного неограниченному кругу лиц.

3.3.5. Обработка ПДн лиц, включенных в кадровый резерв, требует получения их согласия, за исключением случаев нахождения в кадровом резерве действующих работников Учреждения, в трудовом договоре которых определены соответствующие положения. Обязательным является условие ознакомления лица, включаемого в кадровый резерв с условиями ведения кадрового резерва Учреждения, сроком хранения его ПДн, а также порядком его исключения из кадрового резерва.

3.3.6. Обработка ПДн близких родственников работников Учреждения не требует получения их согласия, при условии, что объем обрабатываемых Учреждением ПДн не превышает объем, предусмотренный унифицированной формой № Т-2, утвержденной постановлением Госкомстата РФ от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», либо в случаях, установленных законодательством РФ (получение алиментов, оформление социальных выплат и др.).

3.3.7. Письменное согласие субъекта ПДн на обработку его ПДн в себя включает:

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

– наименование и адрес местонахождения Учреждения;

– цель обработки ПДн;

– перечень ПДн, на обработку которых дается согласие;

– пункт о согласии субъекта ПДн на включение его ПДн в общедоступные источники ПДн (в том числе справочники, адресные книги), с указанием состава включаемых ПДн (при необходимости);

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

– перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых Учреждением способов обработки ПДн;

– срок, в течение которого действует согласие, а также способ его отзыва, если иное не установлено федеральным законом;

– подпись субъекта ПДн.

3.3.8. Получение согласия субъекта ПДн на обработку его ПДн в письменной форме требуется в случае, если:

– Учреждение осуществляет передачу его ПДн третьим лицам, не установленную законодательством РФ;

– Учреждение формирует (организует) общедоступные источники ПДн (в том числе справочники, адресные книги), не установленные законодательством РФ;

– Учреждение намеревается получать его ПДн от третьих лиц, в том числе направлять запросы по прежним местам работы для уточнения или получения дополнительных сведений;

– Учреждение осуществляет обработку специальных категорий ПДн, за исключением случаев, когда обработка специальных категорий ПДн допускается без согласия субъекта ПДн в соответствии с ФЗ «О ПДн»;

– Учреждение осуществляет обработку биометрических ПДн, за исключением случаев, когда обработка биометрических ПДн допускается без согласия субъекта ПДн в соответствии с законодательством РФ о государственной службе, о порядке выезда и въезда в РФ и другими нормативными правовыми актами РФ;

– Учреждение осуществляет трансграничную передачу его ПДн на территории иностранных государств, не обеспечивающих адекватной защиты его прав.

3.3.9. В случаях, предусмотренных законодательством РФ, согласие на обработку ПДн субъекта ПДн дает его законный представитель.

3.3.10. Субъект ПДн имеет право в любое время отозвать данное ранее согласие на обработку его ПДн.

3.3.11. Субъект ПДн имеет право в любое время потребовать от Учреждения исключить сведения о нем из созданных ранее общедоступных источников ПДн (в том числе справочников, адресных книг). Сведения о субъекте ПДн также исключаются из общедоступных источников ПДн по решению суда или иных уполномоченных государственных органов.

3.3.12. Учреждение вправе продолжать обработку ПДн без согласия субъекта ПДн при наличии оснований, установленных законодательством РФ.

3.4. Поручение обработки

3.4.1. Учреждение вправе поручить обработку ПДн другому лицу (далее – уполномоченное лицо) с согласия субъекта ПДн или взять на себя такую обязанность, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия соответствующего акта (далее – поручение).

3.4.2. Поручение предусматривает обязанность уполномоченного лица обеспечить безопасность ПДн при их обработке в ИСПДн уполномоченного лица.

3.4.3. Уполномоченное лицо обязано соблюдать принципы и правила обработки ПДн, предусмотренные ФЗ «О ПДн».

3.4.4. В поручении Учреждения определяется перечень действий (операций) с ПДн, которые будут совершаться уполномоченным лицом, и цели их обработки, а также указываются требования к их защите в соответствии со ст.19 ФЗ «О ПДн».

3.4.5. Уполномоченное лицо не обязано получать согласие субъекта ПДн на обработку его ПДн.

3.4.6. В случае если Учреждение поручает обработку ПДн уполномоченному лицу, ответственность перед субъектом ПДн за действия указанного лица несет Учреждение. Уполномоченное лицо несет ответственность перед Учреждением.

4. ДОСТУП К ПДН

4.1. Доступ работников к ПДн субъектов ПДн

4.1.1. Работники Учреждения получают доступ к ПДн субъектов ПДн исключительно в объеме, необходимом для выполнения своих должностных обязанностей.

4.1.2. Работники Учреждения, получают доступ к ПДн субъектов ПДн исключительно после ознакомления с документами Учреждения, устанавливающими порядок обработки и защиты ПДн.

4.1.3. Список работников, имеющих доступ к ПДн субъектов ПДн на бумажных носителях, определяется Перечнем работников, допущенных к неавтоматизированной обработке ПДн.

4.1.4. Списки работников, имеющих доступ к ресурсам ИСПДн Учреждения, определяются Перечнями прав доступа работников к ресурсам ИСПДн.

4.1.5. Список должностей работников Учреждения, замещение которых предусматривает осуществление обработки ПДн, либо осуществление доступа к ПДн, определяется Перечнем должностей работников, замещение которых предусматривает осуществление обработки ПДн, либо осуществление доступа к ПДн.

4.1.6. Указанные в п.п. 4.1.3-4.1.5 списки, разрабатываются и пересматриваются по мере необходимости (изменение организационно-штатной структуры, введение новых должностей и т.п.) Комиссией на основании заявок руководителей структурных подразделений.

4.1.7. Работнику Учреждения, должность которого не включена в Перечень работников, допущенных к неавтоматизированной обработке ПДн и (или) Перечень прав доступа работников к ресурсам ИСПДн, но которому необходим разовый или временный доступ к ПДн субъектов ПДн в связи с исполнением должностных обязанностей, приказом директора Учреждения предоставляется такой доступ на основании письменного мотивированного запроса непосредственного руководителя работника.

4.1.8. Работник Учреждения получает доступ к ПДн субъектов ПДн после:

– подписания Обязательства работника, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним трудового договора прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей;

– ознакомления и изучения требований настоящего Положения и иных ЛНА Учреждения, регламентирующих защиту и обработку ПДн в части его касающейся;

– прохождения инструктажа о соблюдении правил обработки ПДн, обрабатываемых в Учреждении;

– ознакомления с видами ответственности за нарушение (невыполнение) норм законодательства РФ в сфере обработки и защиты ПДн.

4.1.9. Работники Учреждения, в обязанности которых входит ведение документов, содержащих ПДн субъектов ПДн, обеспечивают каждому субъекту ПДн, возможность ознакомления с документами и материалами, относящимися к нему, если иное не предусмотрено законодательством РФ.

4.2. Доступ субъектов ПДн к своим ПДн

4.2.1. В процессе своей деятельности Учреждение непрерывно взаимодействует с субъектами ПДн в рамках выполнения уставных обязанностей и функций и исполнения договорных обязательств, требуя от субъекта ПДн поддержания своих ПДн в актуальном состоянии.

4.2.2. Субъект ПДн имеет право на получение сведений о наличии у Учреждения его ПДн, а также на ознакомление с ними, в том числе на безвозмездное получение копии любой записи, содержащей его ПДн, за исключением случаев, предусмотренных законодательством РФ.

4.2.3. Субъект ПДн имеет право запрашивать у Учреждения следующие сведения:

– подтверждение факта обработки ПДн Учреждением;

– правовые основания и цели обработки ПДн;

– используемые Учреждением способы обработки ПДн;

– наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с Учреждением или на основании федерального закона;

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

– сроки обработки ПДн, в том числе сроки их хранения;

– порядок осуществления субъектом ПДн прав, предусмотренных законодательством РФ;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

– иные сведения, предусмотренные законодательством РФ.

4.2.4. Право субъекта ПДн на доступ к его ПДн ограничивается, в случае нарушения при таком доступе конституционных прав и свобод других субъектов ПДн.

4.2.5. Право на получение информации, касающейся обработки ПДн, закрепляется за субъектом ПДн с момента заключения договора с Учреждением и действует на протяжении всего срока обработки ПДн (включая хранение), предусмотренного действующим законодательством РФ.

4.2.6. ПДн предоставляются субъекту ПДн или его законному представителю Учреждением при обращении, либо при получении письменного запроса субъекта ПДн или его законного представителя.

4.2.7. Письменный запрос субъекта ПДн должен быть удостоверен следующими документами:

– общегражданским паспортом – в случае непосредственного обращения субъекта ПДн с запросом в Учреждение;

– нотариально заверенной подписью – в случае направления в Учреждение почтового запроса;

– документом, подтверждающим полномочия законного представителя субъекта ПДн – в случае направления в Учреждение запроса от законного представителя субъекта ПДн. При этом непосредственно запрос должен быть удостоверен одним из вышеприведенных способов.

4.2.8. Принципы реагирования на обращения (запросы) субъектов ПДн (их представителей) определяются Правилами рассмотрения запросов субъектов ПДн или их представителей.

4.2.9. ПДн предоставляются субъекту ПДн или его законному представителю в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн.

4.2.10. Все поступившие письменные запросы субъектов ПДн (или их законных представителей) регистрируются ответственным за реагирование на обращения (запросы) субъектов ПДн в Журнале учета обращений (запросов) субъектов ПДн, а затем направляются компетентному работнику для подготовки ответа субъекту ПДн.

4.2.11. Ответ в письменной форме на запрос субъекта ПДн формируется компетентным работником, подписывается директором и отправляется ответственным за реагирование на обращения (запросы) субъектов ПДн в адрес субъекта ПДн через отделение почтовой связи заказным письмом с уведомлением о вручении или курьером (непосредственно в руки адресату под подпись).

4.2.12. Сведения о работниках Учреждения (ФИО, должность и рабочий телефон), которые имеют доступ к ПДн субъектов ПДн, обрабатываемым по поручению третьей стороны, предоставляются субъектам ПДн исключительно при направлении ими письменного запроса в адрес Учреждения.

4.2.13. Субъект ПДн вправе требовать от Учреждения уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

4.2.14. Субъект ПДн при отказе работника Учреждения исключить или исправить неполные, неточные или незаконно полученные ПДн субъекта ПДн имеет право заявить в письменной форме директору Учреждения о своем несогласии, обосновав соответствующим образом такое несогласие. ПДн оценочного характера субъект ПДн имеет право дополнить заявлением, выражающим его собственную точку зрения.

4.3. Доступ третьих лиц к ПДн субъектов ПДн

4.3.1. Доступ третьих лиц к ПДн субъектов ПДн осуществляется только с их письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта ПДн или других лиц, и иных случаев, установленных законодательством РФ, в минимальных объемах и только в целях выполнения задач, соответствующих объективной цели сбора этих данных.

4.3.2. При передаче ПДн субъектов ПДн третьим лицам соблюдаются следующие требования:

– передача осуществляется с согласия субъекта ПДн, за исключением случаев, когда она необходима в целях предупреждения угрозы жизни и здоровью субъекта ПДн, а также в случаях, установленных федеральными законами;

– лица, получающие ПДн субъектов ПДн, предупреждаются о возможности использования полученных сведений лишь в целях, для которых они сообщены, и требуется подтверждение соблюдения этого правила;

– требуется разрешать доступ к ПДн субъектов ПДн только специально уполномоченным лицам, определенных приказом, при этом указанные лица должны иметь право получать только те ПДн субъектов ПДн, которые необходимы им для выполнения должностных обязанностей;

– разрешается предоставлять ПДн субъектов ПДн представителям субъектов ПДн в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми ПДн субъекта ПДн, которые необходимы для выполнения указанными представителями функций.

4.3.3. Не допускается передача сведений, содержащих ПДн субъектов ПДн по открытым (незащищенным) каналам передачи данных, таких как телефон, факс и электронная почта.

4.3.4. Ответы на правомерные письменные запросы других предприятий, учреждений и организаций даются с разрешения директора Учреждения в письменной форме, в том объеме, который позволяет не разглашать излишних ПДн.

4.3.5. Сведения о работнике (в т.ч. уволенном) предоставляются другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

4.3.6. К внешним потребителям ПДн в Учреждении относятся:
– Федеральная налоговая служба России;
– Пенсионный фонд России;
– Органы социального страхования;
– МБУ «Центр обеспечения ФХД» АМО ГО «Сыктывкар»;
– Военкомат;
– Казначейство;
– СЭС;
– Банки;
– Государственные и муниципальные органы власти;
– Территориальные органы федеральных органов исполнительной власти;
– Медицинские организации/лаборатории.

4.4. Общедоступные источники ПДн

4.4.1. Учреждение осуществляет формирование общедоступных источников ПДн на официальном сайте в соответствии с законодательством Российской Федерации.

5. ЗАЩИТА ПДН

5.1. Общие сведения

5.1.1. Учреждение самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения безопасности ПДн, в соответствии с требованиями действующего законодательства РФ в области защиты ПДн.

5.1.2. Кроме мер защиты ПДн, установленных законодательством РФ, Учреждение вправе разрабатывать и внедрять собственные меры защиты ПДн, не противоречащие требованиям законодательства РФ.

5.1.3. В Учреждении принимаются необходимые правовые, организационные и технические меры, обеспечивающие защиту ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении ПДн в соответствии с требованиями к обеспечению безопасности ПДн при их обработке в ИСПДн, установленными Правительством РФ.

5.1.4. Защита ПДн субъектов ПДн от неправомерного их использования или утраты обеспечивается за счет средств Учреждения, в порядке, установленном законодательством РФ.

5.1.5. Защита ПДн представляет собой динамический технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности ПДн и, в конечном счете, обеспечивающий необходимый уровень защищенности, установленный Правительством РФ.

5.1.6. Порядок проведения конкретных мероприятий по защите ПДн с использованием или без использования средств вычислительной техники определяется приказами директора Учреждения и иными ЛНА Учреждения.

5.2. Планирование работ по обеспечению безопасности

5.2.1. В целях исполнения настоящего положения и на основании Положения о постоянно действующей комиссии по защите ПДн и Регламента проведения внутренних мероприятий по контролю обеспечения защиты ПДн, Комиссия ежегодно составляет и утверждает у директора Учреждения Годовой план мероприятий по поддержанию режима защиты ПДн Комиссией.

5.2.2. Проводимые в Учреждении мероприятия по обеспечению безопасности ПДн регистрируются ответственным лицом в Журнале по учету мероприятий по контролю обеспечения защиты ПДн.

5.3. Выполнение работ по обеспечению безопасности

5.3.1. В целях организации и проведения работ по обеспечению безопасности ПДн в Учреждении, приказом директора Учреждения назначаются:

– Комиссия, ответственная за проведение мероприятий по обеспечению безопасности ПДн, поддержание необходимого уровня информационной безопасности и проведение инструктажа работников по основам информационной безопасности при работе с ПДн;

– администратор ИСПДн, ответственный за установку, настройку, администрирование и обслуживание ПО и ТС, применяемых в Учреждении для обработки ПДн.

5.3.2. Комиссия ответственна за проведение следующих мероприятий по обеспечению безопасности ПДн:

– определение и описание ИСПДн;

– определения уровней защищенности ПДн при их обработке в ИСПДн;

– определение актуальных УБПДн;

– проектирование СЗПДн, включающей организационные, физические и технические меры и средства защиты;

– закупку, установку и настройку СЗИ;

– внедрение организационных мероприятий и разработку соответствующих положений, регламентов и инструкций;

– инструктаж и обучение работников, участвующих в обработке ПДн;

– иных мероприятий, установленных Положением о постоянно действующей комиссии по защите ПДн и Регламентом проведения внутренних мероприятий по контролю обеспечения защиты ПДн, а также иными ЛНА Учреждения.

Комиссия для внедрения, настройки и администрирования СЗИ привлекает администратора ИСПДн или стороннюю организацию, имеющую лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Председатель Комиссии назначает лиц из членов Комиссии, ответственных за соблюдение требований настоящего положения и других ЛНА Учреждения, регламентирующих обработку и защиту ПДн.

Для обеспечения безопасности ПДн в Учреждении применяются следующие меры безопасности:

– организационные меры безопасности:

- разграничение прав доступа работников в помещения, выделенные для обработки ПДн, исключающее неконтролируемое пребывание посторонних лиц;
- установление КЗ Учреждения, введение Списка выделенных помещений и Списка лиц, имеющих право самостоятельного доступа в выделенные помещения. Лица, не указанные в Списке, в том числе обеспечивающие техническое и бытовое обслуживание (уборку, ремонт оборудования и технических средств), при наличии необходимости могут посещать выделенные помещения в сопровождении ответственных лиц;
- категорирование ПДн, их хранение и уничтожение в соответствии с требованиями законодательства РФ;
- инструктаж работников по правилам обеспечения безопасности обрабатываемых ПДн;
- учет и хранение МНИ, и порядок их обращения, исключающие хищение, подмену и уничтожение;

- мониторинг и реагирование на инциденты информационной безопасности, связанные с ПДн, включая проведение внутренних проверок, разбирательств и составление заключений;
- постоянный контроль над соблюдением требований по обеспечению безопасности ПДн (реализуется путем внутренних аудитов);
- персональная ответственность работников за нарушение порядка обработки и требований к защите ПДн.

– меры физической безопасности:

- установка металлических дверей входных проемов выделенных помещений;
- установка замков дверей выделенных помещений;
- установка решеток на оконных проемах выделенных помещений первого и последнего этажей зданий Учреждения;
- хранение документов, содержащих ПДн субъектов ПДн в выделенных помещениях, оборудованных запираемыми шкафами и сейфами, обеспечивающими защиту от несанкционированного доступа;
- размещение технических средств, позволяющих осуществлять обработку ПДн, в пределах КЗ;
- организация физической защиты помещений и технических средств, позволяющих осуществлять обработку ПДн.

– технические меры безопасности:

- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- регистрация действий пользователей и обслуживающего персонала, контроль доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- резервирование ТС, дублирование массивов и носителей информации;
- использование защищенных каналов связи;
- разграничение сетевого доступа к ресурсам и АРМ ИСПДн;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

5.3.3. Ремонтно-восстановительные работы проводятся под контролем председателя Комиссии с привлечением администратора ИСПДн. В случае необходимости, ремонт может быть проведен с привлечением сторонних специалистов на договорной основе с составлением актов выполненных работ.

5.4. Контроль выполнения работ по обеспечению безопасности

5.4.1. Контроль выполнения работ по обеспечению безопасности ПДн в Учреждении осуществляется путем проведения периодических контрольных мероприятий (в рамках внутренних аудитов) и внутренних проверок по фактам произошедших инцидентов информационной безопасности.

5.4.2. В рамках проведения контрольных мероприятий выполняется:

– проверка наличия и актуальности планов, регистрационных журналов, актов, договоров, отчетов, протоколов и других свидетельств выполнения мероприятий по обеспечению безопасности ПДн за истекший период;

– проверка осведомленности и соблюдения работниками требований к обеспечению безопасности ПДн;

– проверка соответствия перечня лиц, которым предоставлен доступ к ПДн, фактическому состоянию;

– проверка наличия и исправности функционирования СЗИ, используемых для обеспечения безопасности ПДн, в соответствии с требованиями эксплуатационной и технической документации;

– инструментальная проверка соответствия настроек СЗИ требованиям к обеспечению безопасности ПДн (при необходимости);

– проверка соответствия организационно-распорядительной документации по обеспечению безопасности ПДн действующим требованиям законодательства РФ, руководящих документов ФСБ России, ФСТЭК России.

5.4.3. Все собранные в ходе проведения контрольных мероприятий свидетельства и сделанные по их результатам заключения документируются.

5.4.4. Контрольные мероприятия проводятся как периодически в соответствии с планом и программой аудита, так и внепланово по решению председателя Комиссии, и в случае возникновения инцидентов информационной безопасности.

5.4.5. Внутренние проверки в Учреждении в обязательном порядке проводятся в случае выявления следующих фактов:

– нарушение конфиденциальности, целостности, доступности ПДн;

– халатность и несоблюдение требований по обеспечению безопасности ПДн;

– несоблюдение условий хранения носителей ПДн;

– использование СЗИ, которые могут привести к нарушению заданного уровня безопасности ПДн или к другим нарушениям, приводящим к снижению уровня защищенности ПДн.

5.4.6. Задачами внутренней проверки являются:

– установление обстоятельств нарушения, в том числе времени, места и способа его совершения;

– установление лиц, непосредственно виновных в данном нарушении;

– выявление причин и условий, способствовавших нарушению.

5.5. Совершенствование системы защиты

5.5.1. Ежегодно Комиссия направляет директору Учреждения отчет о проведенных мероприятиях по выполнению Годового плана мероприятий по поддержанию режима защиты ПДн Комиссией, вместе с перечнем предложений по совершенствованию СЗПДн.

5.5.2. Необходимость проведения мероприятий по совершенствованию СЗПДн может быть обусловлена:

– результатами проведенных аудитов и контрольных мероприятий;

– изменениями федерального законодательства в области ПДн;

– изменениями структуры процессов обработки ПДн в Учреждении;

– результатами анализа инцидентов информационной безопасности;

– результатами мероприятий по контролю и надзору за обработкой ПДн, проводимых уполномоченным органом;

– жалобами и запросами субъектов ПДн.

5.5.3. На основании решения, принятого директором Учреждения по результатам рассмотрения ежегодного отчета и предложений по совершенствованию СЗПДн, Комиссия составляет Годовой план мероприятий по поддержанию режима защиты ПДн Комиссией на следующий год.

6. ОТВЕТСТВЕННОСТЬ

6.1. Председатель Комиссии несет персональную ответственность за организацию и поддержание режима защиты ПДн в Учреждении.

6.2. Члены Комиссии несут персональную ответственность за своевременное и качественное исполнение возложенных на них задач и функций в соответствии с ЛНА Учреждения, регламентирующими обработку и защиту ПДн.

6.3. Работники, виновные в нарушении норм обработки и защиты ПДн, определенных законодательством РФ и ЛНА Учреждения несут дисциплинарную, гражданскую, административную, уголовную и иную ответственность, предусмотренную законодательством РФ.

6.4. Разглашение охраняемой законом тайны (государственной, коммерческой, врачебной, служебной и иной), ставшей известной работнику в связи с исполнением трудовых обязанностей, в том числе разглашение ПДн субъектов ПДн, влечет расторжение трудового договора с работником по инициативе работодателя (ст.81 ТК РФ) и наложение административного штрафа на должностное лицо в размере, предусмотренном кодексом РФ об административных правонарушениях (ст.13.14 КоАП РФ).

6.5. Неисполнение или ненадлежащее исполнение работником возложенных на него обязанностей и функций по соблюдению установленного порядка обработки и защиты ПДн влечет замечание, выговор или увольнение работника по соответствующим основаниям (ст.192 ТК РФ).

6.6. Нарушение установленного законом порядка сбора, хранения, использования и распространения ПДн влечет предупреждение или наложение административного штрафа на должностное лицо в размере, предусмотренном кодексом РФ об административных правонарушениях (ст.13.11 КоАП РФ).

6.7. Незаконный сбор или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демострирующемся произведении или средствах массовой информации влечет наказание в соответствии с Уголовным кодексом РФ (ст.137 УК РФ).

6.8. Неправомерный отказ в предоставлении собранных в установленном порядке ПДн, либо предоставление неполных или заведомо ложных сведений, если эти деяния причинили вред правам и законным интересам субъекта ПДн влечет наказание в соответствии с Уголовным кодексом РФ (ст.5.39 КоАП РФ, ст.140 УК РФ).

6.9. Неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в ЭВМ, системе ЭВМ или сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети влечет наказание в соответствии с Уголовным кодексом РФ (ст.272 УК РФ).