ПРИНЯТО
Общим собранием работников
ГБДОУ д/с №22 Кировского района СПб
Протокол №1 от 19.08.2016

УТВЕРЖДЕНО
приказом заведующего ГБДОУ д/с №22
Кировского района СПб №68 п.1 от
22.08.2016 года
_____
/Н.Е.Николаенко/

УЧЕТ МНЕНИЯ ПК
протокол №8 от 19.08.2016
председатель ПК
_____/Е.В.Васильева/

Николаенко Наталья Евгеньевна
Подписано цифровой подписью: Николаенко Наталья Евгеньевна
Дата: 2022.02.26 14:39:21 +03'00'

ПОЛОЖЕНИЕ

О ПОРЯДКЕ ПОЛУЧЕНИЯ, ОБРАБОТКИ, ЗАЩИТЫ И ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ СОТРУДНИКОВ ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ДОШКОЛЬНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ДЕТСКИЙ САД №22 ОБЩЕРАЗВИВАЮЩЕГО ВИДА С ПРИОРИТЕТНЫМ ОСУЩЕСТВЛЕНИЕМ ДЕЯТЕЛЬНОСТИ ПО ПОЗНАВАТЕЛЬНО-РЕЧЕВОМУ РАЗВИТИЮ ДЕТЕЙ КИРОВСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА

Санкт-Петербург

2016 год

1. Общие положения

1.1. Положение о защите и обработке персональных данных в Государственное бюджетное дошкольное образовательное учреждение детский сад №22 общеразвивающего вида с приоритетным осуществлением деятельности по познавательно-речевому развитию детей Кировского района Санкт-Петербурга (далее – Учреждение) устанавливает требования к обеспечению безопасности персональных данных и определяет:

-порядок обработки персональных данных;

-мероприятия по обеспечению защиты прав и свобод граждан при обработке их персональных данных

- ответственность должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.2. Положение разработано в соответствии с:

- Конституцией Российской Федерации;
- Гражданским кодексом Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Указом Президента РФ №188 от 06.09.1997 года «Об утверждении перечня сведений конфиденциального характера»;
- приказом ФСТЭК России от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»;
- Уставом ГБДОУ д/с №22 Кировского района СПб

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

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания или по истечении 75 лет срока их хранения, или продлевается на основании заключения комиссии по защите персональных данных и Учреждения, если иное не определено законом.

2. Основные понятия и состав персональных данных

2.1. Основные понятия, используемые в настоящем Положении:

-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;

-оператор – физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

-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;

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

-использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

-блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

-уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

-обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту 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;

-конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

-трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

-общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.2. Персональные данные, обрабатываемые в Учреждении, содержатся в документах:

- отдела Учреждения делами, кадров;

- отдела бухгалтерского учета и контроля.

2.2.1. В отделе отдела Учреждения делами, кадров создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.2.1.1. документы, содержащие персональные данные работников Учреждения (копия паспорта, копия страхового пенсионного свидетельства, копия ИНН, комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплект материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников, служебных проверок), подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения.

2.2.2. В отделе бухгалтерского учета и контроля создаются и хранятся следующие документы, содержащие данные о работниках в единичном или сводном виде: карточка-справка, копия паспорта, копия страхового пенсионного свидетельства, копия ИНН, копия личного счета для зачисления заработной платы, копии приказов с расчетами, отчеты в органы статистики, отчеты в налоговые органы и другие организации.

3. Порядок сбора и обработки персональных данных

3.1. Порядок получения персональных данных о работниках Учреждения.

3.1.1. Все персональные данные работника Учреждения следует получать 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. Ответственное лицо Учреждения должно 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.

3.1.2. Ответственные лица Учреждения не имеют права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьей 24 Конституции Российской Федерации ответственные лица Учреждения вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Обработка указанных персональных данных работников возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
- по требованию полномочных государственных органов в случаях, предусмотренных федеральными законами.

3.1.3. Письменное согласие работника на обработку своих персональных данных должно включать в себя:

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

-наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

-цель обработки персональных данных;

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

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

-срок, в течение которого действует согласие, а также порядок его отзыва.

Форма заявления о согласии работника на обработку персональных данных – согласно приложения к настоящему Положению.

3.1.4. Согласие работника не требуется в следующих случаях:

-обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

-обработка персональных данных осуществляется в целях исполнения трудового договора;

-обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

-обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

3.2. Порядок обработки, передачи и хранения персональных данных работников Учреждения.

3.2.1. Работник предоставляет ответственным работникам отдела Учреждения делами, кадров и отдела бухгалтерского учета и контроля достоверные сведения о себе. Ответственные работники указанных отделов проверяют достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

3.2.2. В соответствии со статьей 86 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина ответственные работники при обработке персональных данных работника должны соблюдать следующие общие требования:

3.2.2.1. обработка персональных данных 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;

3.2.2.2. при определении объема и содержания, обрабатываемых персональных данных ответственные работники должны руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;

3.2.2.3. при принятии решений, затрагивающих интересы работника, ответственные работники не имеют права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

3.2.2.4. защита персональных данных работника от неправомерного их использования или утраты обеспечивается ответственные работники и за счет средств Учреждения в порядке, установленном нормативными правовыми документами;

3.2.2.5. работники, осуществляющие обработку персональных данных, должны быть ознакомлены под расписку с документами Учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;

3.2.2.6. во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

4. Обеспечение защиты персональных данных

4.1. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

4.2. Безопасность персональных данных при их обработке обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-математических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

4.3. При обработке персональных данных должно быть обеспечено:

-проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

-своевременное обнаружение фактов несанкционированного доступа к персональным данным;

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

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

-постоянный контроль за обеспечением уровня защищённости персональных данных.

4.5. Мероприятия по обеспечению безопасности персональных данных включают в себя:

4.5.1. определение информационных систем, содержащих персональные данные;

4.5.2. классификацию информационных систем персональных данных в соответствии с совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;

4.5.3. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

4.5.4. использование средств защиты информации в соответствии с эксплуатационной и технической документацией;

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

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

4.5.7. учёт лиц, допущенных к работе с персональными данными в информационной системе;

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

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

5. Передача персональных данных

5.1. Передача персональных данных работников Учреждения.

5.1.1. Учреждение не вправе предоставлять 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 случаях, установленных федеральным законодательством.

5.1.2. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника или отсутствует письменное согласие работника на предоставление его персональных сведений, Учреждение обязано отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

5.1.3. Персональные данные работника могут быть переданы представителям третьей стороны в том объёме, в каком это необходимо для выполнения указанными представителями их функций.

5.1.4. Отдел бухгалтерского учёта и контроля Учреждения обрабатывает персональные данные работников Учреждения с целью формирования необходимой электронной отчетности, направляемой в ООО «Сбербанк России», Отделение

Пенсионного Фонда Российской Федерации по Псковской области, Учреждение Федеральной налоговой службы Российской Федерации по Псковской области по защищенным каналам связи.

5.2. При передаче персональных данных работника внутри структурного подразделения или в другое структурное подразделение Учреждения, информация ограничивается только теми персональными данными работника, которые необходимы для выполнения должностными лицами их функции.

5.3. Порядок приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления.

5.3.1. При обнаружении нарушений порядка предоставления персональных данных работник Учреждения должен немедленно приостановить предоставление персональных данных.

5.3.2. Начальник (либо лицо исполняющее его обязанности) Учреждения назначает служебное расследование для выявления причин нарушения.

5.3.3. После устранения нарушений предоставление персональных данных возобновляется.

6. Хранение персональных данных

6.1. Персональные данные работников Учреждения обрабатываются и хранятся в отделе как на бумажных носителях, так и в электронном виде в локальных информационных системах.

7. Доступ к персональным данным

7.1. Доступ работников Учреждения к персональным данным ограничен. В Учреждении вводится разрешительная система доступа к персональным данным, согласно которой разрешается доступ только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

8. Порядок действий должностных лиц в случае обнаружения нарушений, угрожающих конфиденциальности обрабатываемых персональных данных

8.1. В случае обнаружения фактов несоблюдения условий хранения носителей персональных данных, неисправности средств защиты информации, нарушения порядка предоставления персональных данных или иных нарушений, угрожающих конфиденциальности обрабатываемых персональных данных (далее - инцидент информационной безопасности), обнаружившие инцидент работники Учреждения, осуществляющие обработку персональных данных, обязаны немедленно информировать о нем администратору информационной безопасности информационных систем персональных данных Учреждения.

8.2. Предположение о том, что произошел инцидент информационной безопасности, может основываться на следующих признаках:

8.2.1. уведомление антивирусного средства о нарушении информационной безопасности;

8.2.2. сообщение пользователей об отклонениях в работе системных или прикладных программ;

8.2.3. сообщение пользователей о снижении производительности их рабочих станций;

8.2.4. наличие файлов с не читаемыми названиями;

8.2.5. множественные неудачные попытки авторизации.

8.3. Администратором информационной безопасности информационных систем персональных данных Учреждения проводится оценка риска и последствий инцидента, вследствие чего вырабатывается стратегия реагирования на инцидент.

8.4. В случае возможности нарушения конфиденциальности обрабатываемых персональных данных, дальнейшая работа информационных систем прекращается.

8.5. В случае возникновения нарушений на рабочей станции или сервере необходимо произвести полное дублирование информации и проводить работы по расследованию нарушения на отдельном компьютере.

8.6. Электронные журналы должны быть тщательно изучены и проанализированы.

8.7. События инцидента подлежат документированию. Документирование необходимо для сбора и последующего обобщения свидетельств расследования. Документированию подлежат все факты и доказательства злонамеренного воздействия.

8.8. В ходе расследования инцидента все свидетельства должны быть защищены от дискредитации, поскольку данные могут содержать информацию о действенных уязвимостях информационной системы.

8.9. Администратором информационной безопасности информационных систем персональных данных Учреждения составляется заключение по факту инцидента информационной безопасности, включающее в себя:

-исходное протоколирование инцидента;

-причины и следствия возникновения инцидента;

-меры, предпринятые для ликвидации инцидента и его последствий;

-предложения по внесению изменений в систему обеспечения безопасности информации.

9. Обязанности должностных лиц по обеспечению безопасности персональных данных

9.1. Ответственный за организацию работ по защите персональных данных в Учреждении назначается приказом начальника Учреждения.

9.2. Безопасность персональных данных при их обработке обеспечивают должностные лица Учреждения, определенные приказом Учреждения ответственными за осуществление мероприятий по защите персональных данных

9.3. Работники Учреждения, осуществляющие обработку персональных данных в информационных системах, обязаны:

9.3.1. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами информационных систем;

9.3.2. хранить в тайне свой пароль (пароли). В соответствии с разделом 11 настоящего Положения с установленной периодичностью менять свой пароль (пароли);

9.3.3. выполнять требования раздела 12 настоящего Положения в части касающейся действий пользователей рабочих станций информационной системы.

10. Правила учета средств защиты информации и носителей персональных данных

10.1. Средства защиты информации, используемые в информационной системе персональных данных, подлежат учёту в журнале учёта средств защиты информации, в котором отражается:

- наименования средств защиты;
- серийные (заводские) номера;
- наименование организаций, установивших средства защиты;
- место установки средств защиты информации.

10.2. Журнал ведется в электронном виде.

11. Правила парольной защиты

11.1. Пароли должны генерироваться и распределяться централизованно или выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

11.1.1. длина пароля должна быть не менее 6 - 8 символов в зависимости от класса системы;

11.1.2. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы ($, @, #, %, & и другие символы);

11.1.3. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и другие сочетания);

11.1.4. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

11.1.5. личный пароль пользователь не имеет права сообщать никому.

11.2. Работники Учреждения, имеющие доступ к персональным данным, должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

11.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

11.4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 2 месяца.

11.5. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и другие изменения) должна проводиться ответственным за осуществление мероприятий по защите персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.

11.6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие изменения) работников, которым были предоставлены полномочия по управлению парольной защитой.

11.7. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

11.8. Хранение работником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

11.9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за эксплуатацию информационной системы персональных данных, периодический контроль возлагается на ответственного за организацию работ по защите персональных данных.

12. Правила антивирусной защиты

12.1. В Учреждении допускаются к использованию только лицензионные антивирусные средства.

12.2. Установка и настройка параметров средств антивирусного контроля на компьютерах Учреждения осуществляется работниками отдела по обслуживанию рабочих мест Администрации Псковской области

12.3. Ежедневно после включения компьютера (для серверов - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютера.

12.4. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, текстовые файлы любых форматов), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после её приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

12.5. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

12.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка.

12.7. 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.) работник Учреждения самостоятельно или (при необходимости) вместе с работником отдела по обслуживанию рабочих мест Администрации Псковской области внеочередной антивирусный контроль компьютера.

12.8. Ежедневно в автоматическом режиме должно проводиться обновление антивирусных баз.

13. Внутренний контроль организации работ по защите информации

13.1. Внутренняя проверка организации работ по защите информации при их обработке в Учреждении проводится комиссией, состав которой утверждается приказом Учреждения.

13.2 По окончании внутренней проверки организации работ по защите информации составляется протокол, в котором отражаются результаты проверки, выводы и рекомендации по проведению мероприятий, направленных совершенствование организационно-технических мер, необходимых для обеспечения защиты персональных данных в Учреждении (при необходимости вносятся изменения в нормативно-правовые акты Учреждения).

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

Работники Учреждения, виновные в нарушении норм настоящего Положения, а также законодательства Российской Федерации, регулирующего получение, обработку и защиту персональных данных работника, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.