Утверждено
приказом АНО ОДООЦ «Ребячья республика»
от 05.07.2017№ 613

Правила обработки, хранения и уничтожения персональных данных в автономной некоммерческой организации «Областной детский оздоровительно-образовательный центр «Ребячья республика»

1. Общие положения

1.1. Правила обработки, хранения и уничтожения персональных данных в автономной некоммерческой организации «Областной детский оздоровительно-образовательный центр «Ребячья республика» (далее – Правила, АНО ОДООЦ Ребячья республика» далее – Организация) разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Настоящие Правила не исключают обязательного выполнения других руководящих документов по вопросам обработки, передачи, хранения и уничтожения персональных данных.

1.3. Общая ответственность за организацию обеспечения защиты персональных данных возлагается на ответственных лиц за обработку персональных данных, которые назначаются приказом генерального директора Организации.

1.4. Должностные лица, допустившие нарушения требований руководящих и нормативных документов по вопросам защиты персональных данных, привлекаются к ответственности в соответствии с законодательством Российской Федерации.

1.5. По фактам и попыткам несанкционированного доступа к персональным данным, а также случаям утечки персональных данных или утрат машинных носителей информации с персональными данными проводятся служебные расследования.

1.6. В настоящих Правилах используются следующие основные понятия:

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

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

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

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

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

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

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

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

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку технических средств.

2. Общие требования к обработке персональных данных.

2.1. Обработке подлежат только персональные данные, которые отвечают целям их обработки.

2.2. Целями обработки персональных данных являются:

2.2.1. заключение трудовых и иных договоров;

2.2.2. начисление и выплаты заработной платы;

2.2.3. ведение личных карточек сотрудников Организации;

2.2.4. регистрация и обработка сведений о профессиональной служебной деятельности работников Организации;

2.2.5. предоставление сведений в Управление пенсионного фонда Российской Федерации, инспекцию Федеральной налоговой службы Российской Федерации;

2.2.6. регистрация сведений необходимых для надлежащего оказания услуг по организации отдыха и оздоровления детей, а также иных услуг, не противоречащих Уставной деятельности Организации;

2.2.7. предоставление услуг по профессиональному обучению вожатых.

2.3. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.4. В процессе работы с персональными данными работникам запрещается:

2.4.1. разглашать персональные данные в беседах с посторонними лицами, а также с сотрудниками, если этого не требуется для исполнения им своих служебных обязанностей;

2.3.2. выносить носители персональных данных (в том числе бумажные документы) за пределы помещений, если это не связано с выполнением должностных обязанностей работника;

2.4.3. передавать персональные данные по незащищенным каналам связи (в том числе, с использованием общедоступных почтовых серверов типа mail.ru, yandex.ru и прочих);

2.4.4. размещать и хранить персональные данные на ресурсах, не предусмотренных технологическим процессом обработки персональных данных в информационных системах персональных данных (в том числе, сетевых дисках, разделяемых папках, папках Exchange, а также локальных накопителях и жестких дисках компьютера);

2.4.5. подключать к техническим средствам информационных систем персональных данных нештатные устройства ввода-вывода;

2.4.6. использовать неучтенные внешние электронные носители информации;

2.4.7. использовать поступающие из сторонних организаций внешние электронные носители информации без предварительной проверки их на наличие вирусов. При обнаружении на носителе зараженного и не поддающегося лечению файла дальнейшее использование носителя не допускается;

2.4.8. запускать и выполнять посторонние прикладные программы, не предусмотренные технологией работы на компьютере;

2.4.9. обрабатывать персональные данные в случае сбоев в работе средств защиты информации;

2.4.10. использовать ресурсы Интернет (осуществлять обмен сообщениями электронной почты) в случае сбоев в работе средств антивирусной защиты.

3. Порядок обработки персональных данных с использованием средств автоматизации.

3.1. Ответственность за обеспечение защиты персональных данных в информационной системе, возлагается на ответственного за обеспечение безопасности информационных систем персональных данных, который назначается приказом генерального директора.

3.2. Допуск к работе в информационной системе персональных данных осуществляется после ввода её в эксплуатацию и назначения лиц, ответственных за эксплуатацию ПЭВМ в составе информационной системы, предназначенных для обработки персональных данных.

3.3. В информационной системе персональных данных должна соблюдаться парольная защита.

Полная плановая смена паролей пользователей проводится регулярно, не реже одного раза в течение года – в апреле каждого года.

Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу и т. п.) ответственным за обеспечение безопасности информационных систем персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.

Полная внеплановая смена паролей всех пользователей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) ответственным за обеспечение безопасности информационных систем персональных данных.

Хранение должностным лицом значений своих паролей на бумажном носителе допускается только в личном, опечатанном сейфе ответственного за обеспечение безопасности информационных систем персональных данных.

3.4. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.5. Все машинные носители информации, на которых записана информация, содержащая персональные данные субъектов, должны быть зарегистрированы в «Журнале учета машинных носителей информации» (форма в приложении № 1), и иметь этикетку, на которой указывается учетный (регистрационный) номер.

Ответственным лицом за ведение «Журнала учета машинных носителей информации» является главный специалист технической поддержки отдела обеспечения деятельности.

В «Журнале учета машинных носителей информации» учитываются машинные носители филиалов и головного офиса Организации.

Ответственность за наличие этикеток с указанием учетного (регистрационного) номера на машинных носителях информации несет заместитель главного бухгалтера централизованной бухгалтерии.

3.6. При эксплуатации информационной системы, предназначенной для обработки персональных данных, пользователям запрещается:

-вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств информационной системы;

-вносить изменения в состав программного обеспечения, структуру файловой системы без письменного разрешения ответственного за обеспечение безопасности;

-осуществлять попытки несанкционированного доступа к резервам информационной системы и к информации других пользователей;

-подключать информационную систему персональных данных к информационным сетям общего пользования без использования дополнительных средств защиты (сертифицированные межсетевые экраны и средства криптографической защиты данных);

-использовать неучтенные машинные накопители информации.

3.7. При возникновении сбоев в работе информационной системы персональных данных, появления программ-вирусов немедленно сообщить ответственному за обеспечение безопасности информационных систем персональных данных.

3.8. При проведении технического обслуживания и ремонта информационной системы персональных данных, запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения персональных данных. Вышедшие из строя элементы и блоки заменяются на исправные.

3.9. Обязанности работника при обработке персональных данных с использования средств автоматизации:

3.9.1. при работе с персональным компьютером использовать только установленное программное обеспечение, необходимое для выполнения должностных обязанностей работника;

3.9.2. хранить парольную информацию в тайне;

3.9.3. при обработке персональных данных на персональном компьютере, исключить возможность ознакомления с электронными документами посторонних лиц. При отлучении с рабочего места закрывать все электронные документы, базы данных, содержащие персональные данные, блокировать рабочую станцию;

3.9.4. использовать только учтенные внешние электронные носители информации, промаркированные и зарегистрированные ответственным за обеспечение безопасности информационных систем персональных данных (flash-накопители, компакт-диски, дискеты и др.);

3.9.5. в случае необходимости более чем однократного использования электронных носителей информации, полученных из сторонних организаций, учитывать электронные носители в «Журнале учета съемных носителей, полученных от сторонних организаций» (форма в приложении № 2), который заполняет ответственный за обеспечение безопасности информационных систем персональных данных. В случае однократного использования электронного носителя для переноса информации с носителя в информационные системы персональных данных передавать ответственному за обеспечение безопасности информационных систем персональных данных носители для уничтожения;

3.9.6. в нерабочее время внешние электронные носители, содержащие персональные данные, хранить в запирающихся на ключ секциях рабочих столов или в металлических шкафах;

3.9.7. при достижении целей обработки персональных данных, повреждении и выходе из строя носителей сдавать учтенные электронные носители персональных данных для уничтожения главному специалисту технической поддержки - ответственному за обеспечение безопасности информационных систем;

3.9.8. докладывать непосредственному руководителю о нарушениях правил безопасности персональных данных.

4. Порядок обработки персональных данных без использования средств автоматизации.

4.1. Персональные данные при их обработке без использования средств автоматизации, фиксируются на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

4.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

4.3. При использовании типовых форм документов, характер информации в которых предполагается включение в них персональных данных (далее – типовая форма), должно соблюдаться следующее условие: типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, 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.

4.4. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

4.5. Обязанности работников по обработке персональных данных без использования средств автоматизации:

4.5.1. выполнять требования по обеспечению режима конфиденциальности проводимых работ, установленные настоящими Правилами обработки;

4.5.2. обеспечить сохранность бумажных документов в процессе обработки и хранения;

4.5.3. в рабочее/нерабочее время исключать просмотр вверенных документов посторонними людьми, а также работниками Оператора, которым не предоставлен доступ к персональным данным;

4.5.4. использовать документы, содержащие персональные данные, только в рамках должностных обязанностей;

4.5.5. хранить документы на рабочем месте исключительно с целью обработки персональных данных. При достижении целей работы с документами сдавать документы в архив либо осуществлять уничтожение документов с использованием средств уничтожения бумажных носителей.

4.5.6. в нерабочее время бумажные документы хранить в секциях рабочих столов или в запирающихся шкафах.

5. Порядок хранения персональных данных.

5.1. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

5.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

5.3. Персональные данные хранятся:

5.3.1. родителей/законных представителей детей, и детей, отдыхающих в филиалах Организации – у ведущих специалистов, специалистов отдела организации отдыха и оздоровления населения, администратора административно-управленческой службы филиала, работников медицинских служб филиалов;

5.3.2. детей, отдыхающих в филиалах Организации - у ведущих специалистов, специалистов отдела организации отдыха и оздоровления населения, администратора административно-управленческой службы филиала, работников медицинских служб филиалов, работников педагогических служб филиалов;

5.3.3. работников Организации, работающих по трудовым договорам и договорам ГПХ – у специалиста по кадрам отведал делопроизводства, бухгалтера по заработной плате централизованной бухгалтерии;

5.3.4. вожатых, обучающихся в Областной школе подготовки вожатых, преподавателей базового курса Областной школы подготовки вожатых – у методистов научно-методического отдела.

5.4. Машинные носители информации персональных данных в нерабочее время должны храниться в запираемых помещения, в свою очередь съемные носители информации, содержащие персональные данные должны хранится в сейфах или несгораемых шкафах у работников, уполномоченных на обработку персональных данных.

5.5. Работникам, уполномоченным на обработку персональных данных, запрещается:

5.5.1. хранить съемные носители информации, содержащие персональные данные на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам без разрешения генерального директора Организации;

5.5.2. делать несанкционированные копии с носителей персональных данных;

5.5.3. выносить носители с персональными данными за пределы Организации.

6. Передача персональных данных.

6.1. При передаче персональных данных субъекта Оператор должен соблюдать следующие требования:

6.1.1. не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом;

6.1.2. обработка персональных данных субъектов в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия;

6.1.3. предупредить лиц, получивших персональные данные 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, получившие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данные Правила не распространяются на обмен

персональными данными субъектов в порядке, установленном федеральными законами;

6.1.4. оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом о персональных данных. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии с Федеральным законом о персональных данных. Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции;

6.1.5. не запрашивать у субъектов информацию об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни;

6.1.6. передавать персональные данные работников представителям в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

7. Доступ к персональным данным.

7.1. Перечень лиц, имеющих право доступа к персональным данным, определяется приказом генерального директора Организации.

7.2. Субъект персональных данных, чьи персональные данные обрабатываются в информационной системе имеет право:

7.2.1. получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные этого субъекта;

7.2.2. требовать от Оператора уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для оператора персональных данных;

7.2.3. получать от Оператора:

-сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

-перечень обрабатываемых персональных данных и источник их получения;

-сроки обработки персональных данных, в том числе сроки их хранения;

-сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;

7.2.4. требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

7.2.5. копировать и делать выписки персональных данных субъекта разрешается исключительно в служебных целях с письменного разрешения руководителя или заместителя руководителя по кадрам;

7.3. передача информации третьей стороне возможна только при письменном согласии субъектов.

8. Контроль и надзор за выполнением требований настоящих Правил.

8.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и документами АНО ОДООЦ «Ребячья республика», проводятся периодические проверки условий обработки персональных данных. Проверки проводятся ответственными за организацию обработки и обеспечение безопасности информационных систем персональных данных в Организации по плану проведения внутреннего контроля или поручению генерального директора Организации. План проведения внутреннего контроля формируется ответственным за организацию обработки персональных данных и утверждается генеральным директором Организации ежегодно.

8.2. Для проведения проверки создается комиссия, которая состоит из лиц, ответственных за организацию обработки и обеспечение безопасности информационных систем персональных данных.

8.3. Проверки осуществляются путем опроса, а также путем осмотра рабочих мест сотрудников Организации, участвующих в процессе обработки персональных данных.

8.4. Контролируемые вопросы в ходе проведения проверки:

-наличие у сотрудников допуска к обработке персональных данных;

-соблюдение целей, состава и сроков обработки персональных данных;

-соблюдение правил по обезличиванию персональных данных;

порядка доступа в помещения, в которых ведется обработка персональных данных;

-соблюдение сотрудниками правил парольной политики;

-соблюдение сотрудниками правил антивирусной защиты;

-соблюдение сотрудниками правил работы с машинными носителями персональных данных;

-соблюдение порядка работы со средствами защиты информации.

8.4. По итогам каждой проверки составляется протокол проверки соответствия обработки персональных данных требованиям к защите персональных данных по форме, приведенной в Приложении 3 к настоящим Правилам.

8.5. При выявлении в ходе проверки нарушений в протоколе указываются мероприятия по устранению этих нарушений и сроки их исполнения. О результатах проверки и мерах, необходимых для устранения выявленных нарушений, ответственный за организацию обработки персональных данных докладывает генеральному директору Организации.

8.6. Протоколы проверок подписываются ответственными за организацию обработки и обеспечение безопасности персональных данных и утверждаются генеральным директором Организации. Хранятся протоколы проверок у начальника отдела делопроизводства в течение пяти лет.

9. Ответственность за нарушение требований настоящих Правил.

9.1. Правила являются локальным правовым актом, обязательным для выполнения работниками, допущенными к обработке персональных данных.

9.2. На работников возлагается персональная ответственность за невыполнение и/или нарушение требований и положений, установленных настоящими Правилами.

9.3. Работники несут ответственность за сохранность в процессе обработки персональных данных, к которым им разрешен доступ, за сохранность и работоспособное состояние технических, программных средств, носителей персональных данных (в том числе бумажных документов), используемых ими в работе.

9.4. Лица, виновные в нарушении требований настоящих Правил, несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

10. Порядок уничтожения персональных данных.

10.1. Хранение персональных данных должно осуществляться не дольше чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, иным нормативным правовым документом или договором, стороной которого, является субъект персональных данных.

10.2. Уничтожение персональных данных осуществляется комиссией с составлением акта (формы актов в приложении № 4), по истечению сроков хранения и обработки персональных данных.

10.3. Уничтожение бумажных носителей персональных данных осуществляется путем сожжения, либо измельчения в бумаго-уничтожающей машине.

10.4. При необходимости уничтожения части персональных данных, уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению.

10.5. Уничтожение машинных носителей информации производится следующим путем:

-оптические диски и дискеты – путем оплавления в бесформенную массу;

-флешь накопители – путем ударно-механического повреждения основной платы, на которой располагается флешь память;

-накопитель на жестком магнитном диске – путем ударно-механического повреждения исключения возможности восстановления информации в лабораторных условиях.

10.6. Для удаления информации с машинных носителях информации могут использоваться программные методы гарантированного удаления информации, в которых используются основные алгоритмы гарантированного удаления данных.

10.7. Для удаления информации, содержащей персональные данные, из электронных баз данных применяется метод обезличивания персональных данных с целью невозможности определить принадлежность персональных данных конкретному субъекту.

Генеральный директор **Л.В. Шилова**

Приложение 1
к Правилам обработки,
хранения и уничтожения
персональных данных
в АНО ОДООЦ «Ребячья республика»

Журнал учета машинных носителей информации

Начат «___» _____ 20__ года на _____ листах

Окончен «___» _____ 20__ года

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

Учетный номер носителя	Дата регистрации	Вид носителя	Тип носителя	Наименование информации, наносимой на носитель	Отметка о переносе информации на другой носитель	Отметка об отправлении носителя	Отметка о возврате носителя	Отметка об уничтожении (стирании) информации)	Отметка об уничтожении носителя

Расшифровка:

В столбце 1 рядом проставляется номером машинного носителя.
В столбце 2 проставляется информация с указанием числа, месяца и года.
В столбце 3 проставляется: магнитный диск, дискета, оптический диск и др.
В столбце 4 пишется название (марка) носителя.
В столбце 5 указывается наименование информации, которая будет заноситься на носитель, если она заранее известна, если неизвестна, то графа заполняется по мере нанесения информации.

В столбце 6 напротив наименования соответствующей информации проставляются типы носителей, на которые перенесена информация (распечатка, дискета и др.), и их учетные номера.
В столбце 7 проставляются наименование организации, в которую отправлен носитель, наименование, номер и дата сопроводительного документа.
В столбце 8 указываются номер и дата сопроводительного письма, если носитель возвращен с сопроводительным письмом, или порядковый номер и дата поступления пакета с носителем, проставленные в журнале учета поступивших пакетов, если носитель возвращен без сопроводительного письма.
В столбце 9 производится запись "информация уничтожена путем стирания", заверяемая подписью работника, производившего стирание, с проставлением даты. Такие записи должны осуществляться по мере стирания информации и проставляться напротив ее наименования, указанного в графе 5.
Столбец 10 заполняется в том случае, если носитель в силу различных причин уничтожается. При этом указывается способ уничтожения. Отметка об уничтожении носителя заверяется подписями двух работников подразделения несекретного делопроизводства с проставлением даты уничтожения.

Приложение 2
к Правилам обработки,
хранения и уничтожения
персональных данных
в АНО ОДООЦ «Ребячья республика»

Журнал учета съемных носителей информации,
полученных от сторонних организаций.

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	Количество экземпляров	Место использования	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения съемного носителя персональных данных	Сведения об уничтожении съемных носителей персональных данных, стирании информации (подпись, дата)
1									
2									
3									

Приложение 3
к Правилам обработки,
хранения и уничтожения
персональных данных
в АНО ОДООЦ «Ребячья республика»

Протокол проверки соответствия обработки персональных данных требованиям к защите персональных данных в АНО ОДООЦ «Ребячья республика».

Настоящий Протокол составлен о том, что «___» _____ 20__ года (указать должность и Ф.И.О.) – ответственным за организацию обработки персональных данных и (указать должность и Ф.И.О.) – ответственным за обеспечение безопасности персональных данных в АНО ОДООЦ «Ребячья республика», проведена проверка соответствия обработки персональных данных в АНО ОДООЦ «Ребячья республика» требованиям к защите персональных данных.

1. Проверка осуществлялась в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О Персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановлением Правительства Российской Федерации
от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2. В ходе проверки контролировались следующие вопросы:
-наличие у сотрудников допуска к обработке персональных данных;
-наличие согласий субъектов на обработку их персональных данных;
-соблюдение целей, состава и сроков обработки персональных данных;
-соблюдение правил по обезличиванию персональных данных;
-соответствие полномочий сотрудников разрешительной системе доступа к информационным ресурсам, программным и техническим средствам информационной системы персональных данных;
-соблюдение сотрудниками установленной парольной политики;
-соблюдение сотрудниками антивирусной политики;
-соблюдение сотрудниками правил работы со съемными носителями персональных данных;
-соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных;
-соблюдение порядка резервирования баз данных и хранения резервных копий;
-соблюдение порядка работы со средствами защиты информации.

3. В ходе проверки выявлены следующие нарушения:
_____
_____

_____
_____

_____
_____

_____
_____

4. Меры по устранению выявленных нарушений:

_____

_____

_____

Срок устранения выявленных нарушений: «___» _____ 20__ года.

(Должность) – ответственный за организацию обработки персональных данных в АНО ОДООЦ «Ребячья республика» _____ /_____/
(Должность) – ответственный за обеспечение безопасности персональных данных в АНО ОДООЦ «Ребячья республика» _____ /_____/