

УТВЕРЖДАЮ

Заведующий

МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

"11" января 2021 года

П Р А В И Л А

обработки персональных данных в МБДОУ ДС № 16 «Петушок» с. Агой

1. Основные понятия

В настоящем документе используются следующие основные понятия:

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных – состояние защищённости персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических 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;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам;

обработка персональных данных – любое действие (операция) или совокупность действий, 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 (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение 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;

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

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных;

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

2. Общие положения

Настоящие правила разработаны для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных МБДОУ ДС № 16 «Петушок» с. Агой (далее – Учреждение), а также защиты прав и свобод граждан при обработке их персональных данных в Учреждении, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также разъяснение ответственности должностных лиц (служащих), имеющих доступ к персональным данным, за невыполнение требований норм и правил, регулирующих обработку и защиту персональных данных.

Настоящие правила устанавливают порядок обработки персональных данных субъектов персональных данных в Учреждении и направлены на выявление, предотвращение и профилактику нарушений законодательства Российской Федерации в сфере персональных данных.

Субъектами персональных данных в Учреждении являются:

- 1) граждане, обратившиеся за получением услуги.

Настоящие правила определяют необходимый минимальный объём мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к

персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

Настоящие правила разработаны в соответствии со следующими нормативно-правовыми актами Российской Федерации:

1) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года, ратифицированная Федеральным законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" в рамках, определяемых данным Федеральным законом, заявлений;

2) Конституция Российской Федерации;

3) Гражданский кодекс Российской Федерации;

4) Кодекс об Административных Правонарушениях Российской Федерации;

5) Трудовой кодекс Российской Федерации;

6) Уголовный кодекс Российской Федерации;

7) Федеральный закон от 27 июля 2004 года № 79-ФЗ "О государственной гражданской службе Российской Федерации";

8) Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее – Федеральный закон № 152-ФЗ);

9) Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";

10) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 года № 188;

11) Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённое постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687;

12) Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утверждённый постановлением Правительства Российской Федерации от 21 марта 2012 года № 211;

13) Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.

В соответствии с законодательством Российской Федерации об обработке и защите персональных данных персональные данные субъектов являются конфиденциальной информацией.

В случаях, предусмотренных действующим законодательством, сведения о доходах, об имуществе и обязательствах имущественного характера гражданского служащего, его супруги (супруга) и несовершеннолетних детей могут размещаться на официальном сайте Учреждения или предоставляться региональным средствам массовой информации по их запросам для последующего опубликования.

Порядок регистрации, учёта, оформления, тиражирования, хранения, использования и уничтожения документов и других материальных носителей персональных данных определяют законодательство Российской Федерации об обработке и защите персональных данных, а также действующие нормативные правовые акты Учреждения.

Учреждение является оператором персональных данных субъектов, указанных в настоящем документе. На основании соглашения (договора) Учреждение может поручать обработку персональных данных третьим лицам, с согласия субъекта персональных данных, а в случае если иное предусмотрено действующим законодательством Российской Федерации, то и без их согласия. Существенным условием соглашения (договора) по обработке персональных данных является обязанность обеспечения этими лицами конфиденциальности и безопасности персональных данных субъектов.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьёй 24 Конституции Российской Федерации, Учреждение вправе получать и обрабатывать данные о частной жизни гражданских служащих и(или) ов Учреждения только с их письменного согласия.

Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

Настоящие Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами обработки персональных данных.

Все изменения в Правила вносятся приказом Заведующего Учреждения.

3. Цель и содержание обработки персональных данных

Целями обработки персональных данных в Учреждении являются:

1) предоставление государственных и муниципальных услуг.

Цель "предоставление государственных и муниципальных услуг" достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) граждане, обратившиеся за получением услуги:

Иные категории: фамилия, имя, отчество, контактные сведения, адрес.

4. Правила обработки персональных данных

Все персональные данные субъектов Учреждение получает на законной основе.

Персональные данные ближайших родственников (служащих), необходимые для ведения кадрового учёта, Учреждение получает от самих.

Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных. Форма согласия утверждается отдельным приказом.

Субъект персональных данных принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку своей волей и в своём интересе.

Учреждение оставляет за собой право не осуществлять свои функции в отношении субъекта персональных данных в случае предоставления неполных или недостоверных персональных данных, а также в случае отказа дать письменное согласие на обработку персональных данных.

При установлении договорных отношений с субъектом персональных данных получение письменного согласия на обработку его персональных данных не требуется.

Получение персональных данных субъекта у третьих лиц возможно только при предварительном уведомлении субъекта и с его письменного согласия. Форма согласия утверждается отдельным приказом.

Персональные данные субъектов Учреждения обрабатываются в структурных подразделениях в соответствии с исполняемыми функциями.

Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии со списком, утверждённым в порядке, определяемом в Учреждении.

Доступ к персональным данным, обрабатываемым в информационных системах персональных данных, осуществляется в соответствии со списком, утверждённым в порядке, определяемом в Учреждении.

Уполномоченные лица, допущенные к персональным данным субъектов Учреждения, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностными инструкциями указанных лиц.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями "Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" утверждённого Постановлением Правительства РФ от 15 сентября 2008 № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности путём фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются приказом об утверждении мест хранения материальных носителей персональных данных Учреждения.

Персональные данные подлежат уничтожению либо обезличиванию в случаях достижения целей или в случае утраты необходимости в достижении этих целей, отзыва согласия субъекта персональных данных, выявления неправомерной обработки персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения, а также уведомляет субъекта о внесённых изменениях.

Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента отзыва согласия субъекта персональных данных.

Уничтожение персональных данных осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные

являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

Уничтожение персональных данных осуществляется в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных. Учреждение уведомляет об этом субъекта или его законного представителя.

Уничтожение персональных данных на бумажных носителях осуществляет комиссия в составе руководителя и одного структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

- 1) сжигание;
- 2) шредирование (измельчение);
- 3) передача на специализированные полигоны (свалки);
- 4) химическая обработка.

При этом составляется "Акт уничтожения документов Учреждения, содержащих персональные данные субъекта". Форма акта утверждается отдельным приказом.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Учреждения должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, и структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, достигается путём затирания информации на носителях информации (в том числе и резервных копиях) или путём механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных. При этом составляется "Акт уничтожения полей баз данных Учреждения, содержащих персональные данные субъекта". Форма акта утверждается отдельным приказом.

Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определённого срока предусмотрены соответствующими нормативными и (или) договорными документами.

При невозможности осуществления затирания информации на носителях допускается проведение обезличивания путём перезаписи полей баз данных, которые

позволяют определить субъекта, данными, исключая дальнейшее определение субъекта.

Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных в Учреждении.

Обработка биометрических персональных данных (фотография, отпечатки пальцев, сетчатки глаза и другое), в соответствии со статьёй 11 Федерального закона № 152, допускается при наличии согласия субъекта. Форма согласия утверждается отдельным приказом.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

Работники и (служащие) Учреждения должны быть ознакомлены под роспись с требованиями законодательства Российской Федерации, касающимися обработки персональных данных, настоящими Правилами и другими документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

5. Передача персональных данных третьим лицам

При обработке персональных данных субъекта должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта. Форма согласия утверждается отдельным приказом. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащими персональные данные субъекта, при условии соблюдения требований статьи 9 Федерального закона № 152;

2) предупреждать лиц, получающих 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, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Учреждение запрашивает согласие субъекта в письменной форме. Форма согласия утверждается отдельным приказом.

6. Права субъектов персональных данных

В целях обеспечения своих интересов субъекты имеют право:

1) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом;

3) требовать исключения или исправления неверных или неполных персональных

данных, а также данных, обработанных с нарушением Федерального закона № 152-ФЗ. Субъект персональных данных, при отказе Учреждения исключить или исправить персональные данные субъекта, имеет право заявлять в письменной форме о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

4) требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях или исключениях из них;

5) обжаловать в суде любые неправомерные действия или бездействие Учреждения при обработке и защите персональных данных субъекта.

7. Порядок действий в случае запросов надзорных органов

В соответствии с частью 4 статьи 20 Федерального закона № 152 Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных в Учреждении при необходимости с привлечением работников (служащих) Учреждения.

В течение установленного законодательством срока ответственный за организацию обработки персональных данных в Учреждении подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

8. Защита персональных данных субъекта

Защиту персональных данных субъектов от неправомерного их использования или утраты Учреждение обеспечивает за счёт собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1) РД ФСТЭК России – "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года;

2) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282;

3) внутренними документами Учреждения, действующими в сфере обеспечения информационной безопасности.

Защита персональных данных предусматривает ограничение к ним доступа.

Ответственные за организацию обработки персональных данных, администрирование средств и механизмов защиты, техническое обслуживание информационных систем персональных данных назначаются приказом Заведующего

Учреждения.

Руководитель структурного подразделения Учреждения, осуществляющего обработку персональных данных:

1) несёт ответственность за организацию защиты персональных данных в структурном подразделении;

2) организует изучение уполномоченными лицами нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

3) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении (отделе);

4) контролирует порядок доступа к персональным данным в соответствии с функциональными обязанностями в подразделения.

и (служащие), допущенные к персональным данным дают письменное обязательство о неразглашении таких данных.

9. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с персональными данными, обязаны:

1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Учреждения по защите персональных данных;

2) сохранять конфиденциальность персональных данных;

3) обеспечивать сохранность закреплённых за ними носителей персональных данных;

4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

5) докладывать своему непосредственному руководителю структурного подразделения обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

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

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности в соответствии с действующим законодательством Российской Федерации.

К данным лицам могут быть применены следующие дисциплинарные взыскания:

1) замечание;

2) выговор;

3) предупреждение о неполном должностном соответствии;

4) увольнение с гражданской службы.

Заведующий
МБДОУ ДС № 16 «Петушок» с.Агой



Л.В. Ткаченко

УТВЕРЖДАЮ

Заведующий

МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

"11" января 2021 года

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ ДС № 16 «Петушок» с. Агой

1. Общие положения

Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" и требованиями по соблюдению мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденных постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях МБДОУ ДС № 16 «Петушок» с. Агой (далее – Учреждение).

Правила обязательны для исполнения всеми должностными лицами Учреждения, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях Учреждения осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в структурных подразделениях, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных в Учреждении.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов министерства или нарушения требований по обработке и защите персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в Учреждении либо комиссией, образуемой Заведующим Учреждения.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений (отделов).

Периодичность и сроки проведения плановых проверок подразделений Учреждения устанавливаются планом, утверждаемым Заведующим Учреждения. Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа Заведующего Учреждения. Ответственный за организацию обработки персональных данных в Учреждении подготавливает предложения по составу комиссии. Проект приказа о проверке подготавливает ответственный за организацию обработки персональных данных в Учреждении.

Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

3. Порядок проведения проверки

По прибытию в структурное подразделение для проведения проверки председатель комиссии прибывает к руководителю проверяемого структурного подразделения Учреждения, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии по проверке и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления субъектов проверяемого структурного подразделения со своей ответственностью;

2) получение при содействии субъектов проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц структурного подразделения необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в проверяемом структурном подразделении Учреждения рассматриваются в частности следующие показатели:

1) в части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных и в положении о порядке обработки персональных данных Учреждения, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в Учреждении;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов работниками (служащими), имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов Учреждения работниками (служащими), имеющими доступ к персональным данным;

е) наличие документов, определяющих состав ов, ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных работников с данными документами;

ж) уровень подготовки работников, ответственных за организацию защиты персональных данных в подразделении;

з) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.

2) в части защиты персональных данных в информационных системах персональных данных (далее - ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

з) тестирование реализации правил фильтрации межсетевое экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевое экрана, процесса регистрации действий администратора межсетевое экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевое экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность установления уровня защищенности персональных данных в информационной системе;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о структурных подразделениях Учреждения, должностных инструкциях ов (служащих) и трудовых договорах;

г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных

документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

- 1) актом - при проведении проверки комиссией;
- 2) служебной запиской - при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах и подписывается членами комиссии.

Один экземпляр хранится у ответственного за организацию обработки персональных данных Учреждения. Второй экземпляр хранится в Учреждении в установленном порядке. Копия акта о проверке остается в проверяемом структурном подразделении.

Результаты проверок структурных подразделений периодически обобщаются ответственным за организацию обработки персональных данных в Учреждении и доводятся до руководителей структурных подразделений. При необходимости принятия решений по результатам проверок структурных подразделений на имя Заведующего Учреждения готовятся соответствующие служебные записки.

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

У Т В Е Р Ж Д А Ю

Заведующий

МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко

"11" января 2021 года

ПРАВИЛА

работы с обезличенными данными в МБДОУ ДС № 16 «Петушок» с. Агой

Настоящие правила разработаны в соответствии с положениями Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных" и требованиями по соблюдению мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утверждённых постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяют порядок работы с обезличенными данными в структурных подразделениях (отделах) МБДОУ ДС № 16 «Петушок» с. Агой (далее – Учреждение).

Правила обязательны для исполнения всеми должностными лицами Учреждения, допущенными к персональным данным.

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

Персональные данные подлежат уничтожению либо обезличиванию в случаях достижения целей обработки или в случае утраты необходимости в их достижении.

Порядок обезличивания включает в себя замену идентифицирующей информации о субъекте, например, одновременно фамилии, имени и отчества на произвольный код (далее – идентификатор).

В случае, если обезличенные персональные данные используются в статистических или иных исследовательских целях, сроки обработки и хранения персональных данных устанавливаются руководством Учреждения исходя из служебной необходимости, получение согласия субъекта на обработку его персональных данных в данном случае не требуется на основании пункта 9 части 1 статьи 6 Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных".

Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных персональных данных в информационных системах и целесообразность их применения определяются

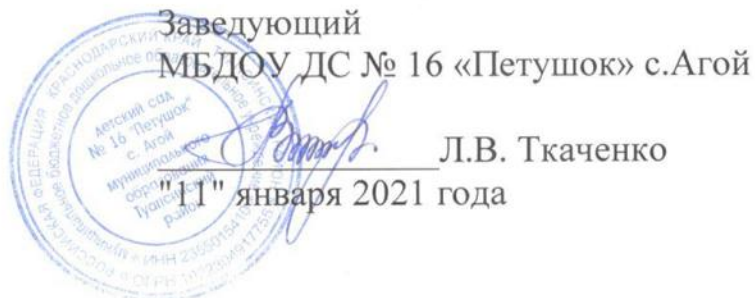
ответственным за организацию обработки персональных данных в Учреждении индивидуально для каждой информационной системы персональных данных.

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

УТВЕРЖДАЮ



Заведующий

МБДОУ ДС № 16 «Петушок» с.Агой

Л.В. Ткаченко

"11" января 2021 года

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в МБДОУ ДС № 16 «Петушок» с. Агой в связи с реализацией трудовых отношений

1. Фамилия, имя, отчество, дата и место рождения, гражданство.
2. Образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому).
3. Послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), учёная степень, учёное звание (когда присвоены, номера дипломов, аттестатов).
4. Выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность).
5. Государственные награды, иные награды и знаки отличия (кем награждён и когда).
6. Места рождения, места работы и домашние адреса близких родственников (отца, матери, братьев, сестёр и детей), а также мужа (жены).
7. Пребывание за границей (когда, где, с какой целью).
8. Адрес регистрации и фактического проживания.
9. Дата регистрации по месту жительства.
10. Паспортные данные (серия, номер, кем и когда выдан).
11. Номер телефона.
12. Отношение к воинской обязанности, сведения по воинскому учёту (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу).
13. Идентификационный номер налогоплательщика.
14. Номер страхового свидетельства обязательного пенсионного страхования.
15. Наличие (отсутствие) судимости.

Заведующий

A blue ink signature of L.V. Tkachenko.

Л.В. Ткаченко

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН**

ПРИКАЗ

11.01. 2021 г.

№ 26/6 - О

с. Агой

О назначении ответственных лиц за сбор, обработку, хранение персональных данных в МБДОУ ДС №16 «Петушок» с. Агой МО Туапсинский район

В соответствии с гл.14 Трудового кодекса РФ, Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных", других действующих нормативно-правовых актов РФ, в целях обеспечения соблюдения трудового законодательства и иных нормативно-правовых актов п р и к а з ы в а ю:

1. Назначить ответственных за сбор, хранение, обработку и передачу персональных данных следующих сотрудников:

- старшего воспитателя – Остроухову Сюзанну Николаевну;
- заведующего ДОУ – Ткаченко Людмилу Васильевну;
- медицинскую сестру – Бабаян Наталию Владимировну;
- председателя профсоюзного комитета – Куадже Диану Сергеевну;
- заведующего хозяйством – Пирогову Ольгу Викторовну.

2. Контроль за исполнением приказа оставляю за собой.

Заведующий



Л.В. Ткаченко

С приказом ознакомлены, согласны:

Ф.И.О.	Должность	Подпись
Остроухова Сюзанна Николаевна	старший воспитатель	
Бабаян Наталия Владимировна	медицинская сестра	
Куадже Диана Сергеевна	председателя профсоюзного комитета	
Пирогова Ольга Викторовна	заведующий хозяйством	

УТВЕРЖДАЮ

Заведующий
МБДОУ ДС № 16 «Петушок» с.Агой



Л.В. ткаченко

"11" января 2021 года

ПЕРЕЧЕНЬ

должностей служащих МБДОУ ДС № 16 «Петушок» с. Агой, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1	Медицинский	Старшая медицинская сестра
2	Администрация	Заведующий хозяйством
3	Педагогический	Старший воспитатель, Учитель - логопед

Заведующий

Л.В. Ткаченко

УТВЕРЖДАЮ



Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко

«11» января 2021 года

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в МБДОУ ДС
№ 16 «Петушок» с. Агой

1. Общие положения

Ответственный за организацию обработки персональных данных (далее – Ответственный) является работником МБДОУ ДС № 16 «Петушок» с. Агой (далее – Учреждение).

Ответственный назначается приказом Заведующего Учреждения.

Ответственный в вопросах организации обработки персональных данных подчиняется непосредственно Заведующему и проводит мероприятия по защите персональных данных в интересах Учреждения.

Ответственный в своей деятельности руководствуется:

- 1) Конституцией Российской Федерации;
- 2) Федеральными законами Российской Федерации и нормативными правовыми актами органов государственной власти по вопросам защиты персональных данных;
- 3) Государственными стандартами Российской Федерации в области защиты информации;
- 4) Руководящими и нормативными правовыми документами Федеральной Службы по техническому и экспортному контролю России;
- 5) Локальными нормативными актами Учреждения по защите персональных данных;
- 6) Правилами внутреннего трудового распорядка.

Деятельность Ответственного осуществляется согласно плану мероприятий по защите персональных данных Учреждения на год.

2. Задачи

На Ответственного возложены следующие задачи:

1) организация внутреннего контроля за соблюдением работниками (служащими) Учреждения норм законодательства Российской Федерации по обработке персональных данных, в том числе требований, предъявляемых к защите персональных данных;

2) разработка, внедрение и актуализация локальных актов по вопросам обработки персональных данных;

3) доведение до сведения работников (служащих) Учреждения, непосредственно осуществляющих обработку персональных данных, положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных, и проведение обучения указанных ов;

4) осуществление контроля приёма и обработки обращений и запросов субъектов персональных данных или их законных представителей по вопросам обработки персональных данных и внесение предложений по организации приёма и обработки таких обращений и запросов;

5) осуществление рассмотрения обращений и запросов субъектов персональных данных или их законных представителей по вопросам обработки персональных данных и организация предоставления субъектам персональных данных или их законным представителям информации,

предусмотренной Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных";

б) организация комплексной защиты объектов информатизации Учреждения, а именно:

а) информационных ресурсов, представленных в виде документированной информации на магнитных, оптических носителях, информативных физических полей, информационных массивов и баз данных, содержащих персональные данные субъектов Учреждения;

б) средств и систем информатизации (средств вычислительной техники, информационно-вычислительных комплексов, локальных вычислительных сетей и корпоративных информационных систем), программных средств (операционных систем, систем управления базами данных, другого общесистемного и прикладного программного обеспечения), автоматизированных систем управления информационными, управленческими и технологическими процессами, систем связи и передачи данных, технических средств приёма, передачи и обработки информации (звукозаписи, звукоусиления, звуковоспроизведения, переговорных устройств и других технических средств обработки графической, смысловой и буквенно-цифровой информации), используемых для реализации процессов ведения деятельности, обработки информации, содержащей персональные данные субъектов Учреждения.

7) организация защиты персональных данных субъектов Учреждения;

8) разработка и проведение организационных мероприятий, обеспечивающих безопасность объектов защиты Учреждения, своевременное выявление и устранение возможных каналов утечки информации;

9) организация проведения работ по технической защите информации на объектах информатизации, в информационно-вычислительных сетях, системах и средствах связи и телекоммуникаций Учреждения;

10) реализация технических мер, обеспечивающих своевременное выявление возможных технических каналов утечки информации в структурных подразделениях (отделах) Учреждения;

11) методическое руководство системой обеспечения информационной безопасности Учреждения;

12) организация контроля состояния и проведение оценки эффективности системы обеспечения информационной безопасности персональных данных, а также реализация мер по её совершенствованию;

13) внедрение в информационную инфраструктуру Учреждения современных методов и средств обеспечения информационной безопасности.

3. Функции

Для решения поставленных задач Ответственный осуществляет следующие функции:

1) участие в разработке и внедрении правовых, организационных и технических мер по комплексному обеспечению безопасности персональных данных;

2) контроль обеспечения соблюдения режима конфиденциальности при обработке персональных данных и внесение предложений по соблюдению такого режима;

3) разработка планов по защите персональных данных на объектах Учреждения;

4) контроль выполнения мер по защите персональных данных, анализ материалов контроля, выявление недостатков и нарушений. Разработка и реализация мер по их устранению;

5) контроль выполнения плановых заданий, договорных обязательств, а также сроков, полноты и качества работ по защите персональных данных, выполняемых контрагентами;

6) разработка и внесение предложений по обеспечению финансирования работ по защите персональных данных, в том числе выполняемых по договорам;

7) участие в проведении работ по технической защите информации на объектах информатизации Учреждения. Оценка эффективности принятых мер по технической защите информации;

8) внесение предложений по обеспечению выбора, установке, настройке и эксплуатации средств защиты информации в соответствии с организационно-распорядительной и

эксплуатационной документацией;

9) контроль организации режима обеспечения безопасности помещений, в которых происходит обработка персональных данных, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в такие помещения, а также внесение предложений по обеспечению безопасности таких помещений;

10) участие в организации доступа работников (служащих) Учреждения к персональным данным в соответствии с возложенными на них должностными обязанностями и подготовка предложений по организации такого доступа;

11) разработка и внедрение локальных актов, определяющих перечень работников Учреждения, имеющих доступ к персональным данным;

12) контроль размещения устройств ввода (отображения) информации, исключающего её несанкционированный просмотр;

13) проведение оценки вреда, который может быть причинён субъектам персональных данных в случае нарушения законодательства по защите персональных данных;

14) участие в разработке и реализации политики по работе с инцидентами информационной безопасности, в части обработки персональных данных;

15) внесение предложений по актуализации внутренней организационно-распорядительной документации по защите персональных данных при изменении существующих и выходе новых нормативных правовых документов по вопросам обработки персональных данных и подготовка соответствующих необходимых проектов документов.

4. Права

Ответственный имеет право:

1) осуществлять контроль за деятельностью структурных подразделений (отделов) Учреждения по выполнению ими требований по защите персональных данных;

2) составлять акты, докладные записки, отчёты для рассмотрения руководством Учреждения, при выявлении нарушений порядка обработки персональных данных;

3) принимать необходимые меры при обнаружении несанкционированного доступа к персональным данным, как работниками (служащими) Учреждения, так и третьими лицами, и докладывать о принятых мерах Заведующему Учреждения с предоставлением информации о субъектах, нарушивших режим доступа;

4) вносить на рассмотрение Заведующему Учреждения предложения, акты, заключения о приостановлении работ в случае обнаружения каналов утечки (или предпосылок к утечке) информации ограниченного доступа;

5) давать структурным подразделениям (отделам) Учреждения, а также отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного;

6) запрашивать и получать от всех структурных подразделений (отделов) Учреждения сведения, справочные и другие материалы, необходимые для осуществления деятельности Ответственного;

7) составлять акты и другую техническую документацию о степени защищённости объектов информатизации;

8) готовить и вносить предложения: на проведение работ по защите персональных данных; о привлечении к проведению работ по оценке эффективности защиты персональных данных на объектах Учреждения (на договорной основе) учреждений и организаций, имеющих лицензию на соответствующий вид деятельности; о закупке необходимых технических средств защиты и другой спецтехники, имеющих в обязательном порядке сертификат соответствия;

9) осуществлять визирование договоров с контрагентами с целью правового обеспечения передачи им персональных данных субъектов Учреждения в ходе выполнения работ по этим договорам;

10) представлять интересы Учреждения при осуществлении государственного контроля и

надзора за обработкой персональных данных Уполномоченным органом по защите прав субъектов персональных данных.

5. Взаимоотношения (служебные связи)

Ответственный выполняет свои задачи осуществляя взаимодействие со всеми структурными подразделениями (отделами) Учреждения.

Для выполнения своих функций и реализации предоставленных прав Ответственный взаимодействует с территориальными и региональными подразделениями Федеральной службы по техническому и экспортному контролю России, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, Федеральной службы безопасности Российской Федерации, Министерства внутренних дел Российской Федерации и другими представителями исполнительной власти и организациями, предоставляющими услуги и выполняющими работы в области защиты персональных данных на законном основании.

6. Ответственность

Ответственный несёт ответственность за надлежащее и своевременное выполнение возложенных задач и функций по организации обработки персональных данных в Учреждении в соответствии с положениями законодательства Российской Федерации в области персональных данных.

Заведующий



Л.В. Ткаченко

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН**

ПРИКАЗ

11.01.2021 г.

№ 26 - О

с. Агой

Об организации работы МБДОУ ДС №16 «Петушок» с. Агой в
автоматизированной системе «Сетевой город. Образование»,
автоматизированной информационной системе «Е-услуги. Образование»
в 2021 году

В соответствии Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных", Федеральным законом от 27.07.2010 года № 210 – ФЗ «Об организации предоставления государственных и образовательных услуг», в целях формирования единого информационно - образовательного пространства системы образования, организации мониторинга и контроля для обеспечения полноты, достоверности и актуальности баз данных автоматизированной системы «Сетевой город. Образование» и автоматизированной информационной системы «Е-услуги. Образование» (далее – АИС «СГО», «Е-услуги») п р и к а з ы в а ю:

1. Назначить ответственных операторов за АИС «СГО», «Е-услуги» следующих сотрудников:

- старшего воспитателя – Остроухову Сюзанну Николаевну;
- заведующего ДОУ – Ткаченко Людмилу Васильевну.

2. Ответственным операторам вменить полномочия по своевременному и правильному заполнению разделов и оперативной работе в системах АИС «СГО» и «Е-услуги».

3. Ответственность за достоверность данных в в системах АИС «СГО» и «Е-услуги». и контроль по исполнению настоящего приказа оставляю за собой.

Заведующий



Л.В. Ткаченко

С приказом ознакомлены, согласны:

С.Н. Остроухова

Л.В. Ткаченко

Заведующему МБДОУ ДС № 16 «Ягодка»
с. Агой МО Туапсинский район

Ткаченко Л.В.

**Заявление-согласие
субъекта на обработку его персональных данных**

Я, _____,
паспорт серии _____, номер _____, выдан _____

_____ года, в соответствии с Федеральным законом от 27.07.2006 г.
№ 152-ФЗ "О персональных данных" частью 1 статьи 6 главы 2, даю согласие МБДОУ ДС
№ 16 «Петушок» с. Агой, расположенному по адресу 352830, Туапсинский район, с. Агой ул.
Центральная 14Г, на обработку моих персональных данных, а именно:

- | | | |
|---|---|--------------------------------------|
| <input type="checkbox"/> ФИО | <input type="checkbox"/> Адрес | <input type="checkbox"/> Образование |
| <input type="checkbox"/> Дата рождения | <input type="checkbox"/> Паспортные данные | <input type="checkbox"/> ИНН |
| <input type="checkbox"/> Место рождения | <input type="checkbox"/> Семейное положение | <input type="checkbox"/> Профессия |
| <input type="checkbox"/> другие: _____ | | |

(перечислить дополнительные категории персональных данных)

Перечень действий, осуществляемых с персональными данными: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение, в целях осуществления персонального учета в системе государственного страхования и других целях, определенных законодательством Российской Федерации, осуществляет смешанную обработку персональных данных с применением ЭВМ.

Согласие вступает в силу со дня его подписания и действует в течение срока хранения персональных данных. Действие настоящего согласия прекращается досрочно в случае принятия оператором решения о прекращении обработки персональных данных и/или уничтожения документов содержащих персональные данные.

Согласие может быть отозвано мною в любое время на основании моего письменного заявления, не менее чем за 2 недели до момента отзыва согласия.

"__" _____ 20__ г.

(подпись)

УТВЕРЖДАЮ

Заведующий

МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

11 января 2021 года

ПОРЯДОК

доступа служащих МБДОУ ДС № 16 «Петушок» с. Агой в помещения, в которых ведётся обработка персональных данных

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а также обеспечения внутриобъектового режима.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нестандартных ситуациях.

Объектами охраны МБДОУ ДС № 16 «Петушок» с. Агой (далее – Учреждение) являются:

1) помещения, в которых происходит обработка персональных данных как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;

2) помещения, в которых хранятся материальные носители персональных данных и резервные копии персональных данных;

3) помещения, в которых установлены криптографические средства, предназначенные для шифрования персональных данных, в том числе носители ключевой информации (далее спецпомещения).

Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются и Учреждения, не допущенные к обработке персональных данных и лица, не являющиеся амами Учреждения.

К спецпомещениям, предъявляются дополнительные требования по безопасности, указанные в разделе 4.

Ответственность за соблюдение положений настоящего порядка несут и структурных подразделений, допущенные в помещения, являющиеся объектами охраны, а также их руководители.

Контроль соблюдения требований настоящей инструкции обеспечивает, назначенный ответственным за организацию обработки персональных данных в Учреждении.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

Например: металлические решётки на окнах, металлическая дверь, система контроля и управления доступа и так далее.

2. Правила доступа в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведётся обработка персональных данных, а также хранятся материальные носители персональных данных и резервные копии персональных данных, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица, из числа работников, допущенных к обработке персональных данных.

При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведётся обработка персональных данных лиц из числа ов Учреждения, не допущенных к обработке персональных данных.

В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведётся обработка персональных данных, должны быть надёжно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

Доступ работников в помещения, в которых ведётся обработка персональных данных в нерабочее время, допускается по распоряжению руководства Учреждения.

3. Правила доступа в серверные помещения

Доступ в серверные помещения, в которых ведётся обработка персональных данных осуществляется в соответствии со списком, утверждённым в Учреждении.

Уборка серверных помещений происходит только под контролем лица, из указанных в утверждённом списке.

Доступ в серверные помещения посторонних лиц допускается по согласованию с ответственным за обеспечение безопасности информационных систем персональных.

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем персональных.

Доступ ов в серверные помещения в нерабочее время допускается по распоряжению руководства Учреждения.

4. Правила доступа в спецпомещения

Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также опечатывание спецпомещений по окончании рабочего дня или оборудование спецпомещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии спецпомещений.

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утверждённым приказом Заведующего Учреждения.

Доступ иных лиц в спец помещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий

нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц их числа работников Учреждения.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Учреждения.

При утрате ключа от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Доступ работников в спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов), подписанных Заведующим Учреждения.

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН

ПРИКАЗ

11.01. 2021 г.

№ 26/1 - О

с. Агой

О создании комиссии по проведению периодических проверок
МБДОУ ДС № 16 «Петушок» с. Агой МО Туапсинский район

В соответствии с Федеральным закона Российской Федерации от
27 июля 2006 года № 152-ФЗ «О персональных данных» п р и к а з ы в а ю:

4. Назначить комиссию по проведению внутренних
периодических проверок по обработки персональных данных в
составе:

Ткаченко
Людмила Васильевна - Заведующий, председатель
комиссии;

Пирогова
Ольга Викторовна - Заведующей хозяйством;

Куадже
Диана Сергеевна - председатель профсоюзного
комитета;

Бабаян
Наталия Владимировна - Старшая медицинская сестра.

2. Комиссии в своей работе руководствоваться требованиями к защите
персональных данных при их обработке в информационных системах
персональных данных, утвержденными постановлением Правительства
Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении
требований к защите персональных данных при их обработке в
информационных системах персональных данных».

3. Комиссии по результатам работ ежеквартально предоставить
Заведующему на утверждение акты (Приложение № 1)

4. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий



Л.В. Ткаченко

УТВЕРЖДАЮ

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

2017 года

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ ДС № 16 «Петушок» с. Агой МО Туапсинский район

1. Общие положения

Настоящие правила разработаны в соответствии с положениями Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных" и требованиями по соблюдению мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утверждённых постановлением Правительства Российской Федерации от 21 марта 2012 года № 211, и определяют порядок организации и осуществления контроля выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях МБДОУ ДС № 16 «Петушок» с. Агой (далее – Учреждение).

Правила обязательны для исполнения всеми должностными лицами Учреждения, осуществляющими контроль состояния защиты персональных данных.

Контроль выполнения соответствия обработки персональных данных требованиям к защите персональных данных в структурных подразделениях Учреждения осуществляется с целью определения наличия несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, правильности обработки персональных данных ответственными лицами в структурных подразделениях, а также выработать меры по их устранению и недопущению в дальнейшем.

Контроль осуществляет ответственный за организацию обработки персональных данных в Учреждении.

Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

Контрольные проверки проводятся для установления полноты

выполнения рекомендаций плановых проверок.

Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов министерства или нарушения требований по обработке и защите персональных данных.

Проверки осуществляются ответственным за организацию обработки персональных данных в Учреждении либо комиссией, образуемой Заведующим Учреждения.

Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений не позднее, чем за 24 часа до начала проверки.

Проверки по частным вопросам могут проводиться без уведомления руководителей проверяемых подразделений (отделов).

Периодичность и сроки проведения плановых проверок подразделений Учреждения устанавливаются планом, утверждаемым Заведующим Учреждения. Сроки проведения плановых проверок доводятся руководителям проверяемых структурных подразделений (отделов) не позднее, чем за 10 суток до начала проверки.

2. Порядок подготовки к проверке

Проверка проводится на основании приказа Заведующего Учреждения. Ответственный за организацию обработки персональных данных в Учреждении подготавливает предложения по составу комиссии. Проект приказа о проверке подготавливает ответственный за организацию обработки персональных данных в Учреждении.

Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения.

3. Порядок проведения проверки

По прибытию в структурное подразделение для проведения проверки председатель комиссии прибывает к руководителю проверяемого структурного подразделения Учреждения, представляется ему и представляет других прибывших на проверку лиц.

Руководитель проверяемого структурного подразделения обязан оказывать содействие комиссии по проверке и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

На период проведения контрольных мероприятий обработку персональных данных необходимо по возможности прекращать. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым

сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

Общий порядок проведения проверки включает следующее:

1) получение документов о распределении обязанностей по обработке и защите персональных данных, выявление ответственных за обработку и защиту персональных данных и установление факта ознакомления ов проверяемого структурного подразделения со своей ответственностью;

2) получение при содействии ов проверяемого структурного подразделения документов, касающихся обработки и защиты персональных данных в данном структурном подразделении;

3) анализ полученной документации;

4) непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

При этом согласовываются конкретные вопросы по объёму, содержанию, срокам проведения проверки, а также каких должностных лиц структурного подразделения необходимо привлечь к проверке и какие объекты следует посетить.

В ходе осуществления контроля выполнения требований по обработке и защите персональных данных в проверяемом структурном подразделении Учреждения рассматриваются в частности следующие показатели:

1) в части общей организации работ по обработке персональных данных:

а) соответствие информации, указанной в уведомлении об обработке персональных данных и в положении о порядке обработки персональных данных Учреждения, реальному положению дел;

б) соответствие обрабатываемой и собираемой информации (персональных данных), их полнота, в соответствии с нормативными правовыми актами и локальными актами, принятыми в Учреждении;

в) наличие нормативных документов по защите персональных данных;

г) знание нормативных документов ами (служащими), имеющими доступ к персональным данным;

д) полнота и правильность выполнения требований нормативных документов Учреждения ами (служащими), имеющими доступ к персональным данным;

е) наличие документов, определяющих состав ов, ответственных за организацию защиты персональных данных в подразделении, соответствие этих документов реальному штатному составу подразделения, а также подтверждение факта ознакомления ответственных ов с данными документами;

ж) уровень подготовки ов, ответственных за организацию защиты персональных данных в подразделении;

з) наличие согласий на обработку персональных данных субъектов персональных данных. Соответствие объёма персональных данных и сроков обработки целям обработки персональных данных.

2) в части защиты персональных данных в информационных системах

персональных данных (далее - ИСПДн):

а) соответствие средств вычислительной техники ИСПДн показателям, указанным в документации на ИСПДн;

б) структура и состав локальных вычислительных сетей, организация разграничения доступа пользователей к сетевым информационным ресурсам, порядок защиты охраняемых сведений при передаче (обмене) персональных данных в сети передачи данных;

в) соблюдение установленного порядка использования средств вычислительной техники ИСПДн;

г) наличие и эффективность применения средств и методов защиты персональных данных, обрабатываемых на средствах вычислительной техники;

д) соблюдение требований, предъявляемых к паролям на информационные ресурсы;

е) соблюдение требований и правил антивирусной защиты средств вычислительной техники;

ж) контроль журналов учёта носителей персональных данных. Сверка основного журнала с дублирующим (если требуется ведение дублирующего учёта носителей);

з) тестирование реализации правил фильтрации межсетевого экрана, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления настроек межсетевого экрана.

3) в части защиты информационных ресурсов и помещений:

а) правильность отнесения обрабатываемой информации к персональным данным;

б) правильность установления уровня защищенности персональных данных в информационной системе;

в) закрепление гражданско-правовой ответственности в сфере информационной безопасности и соблюдения режима конфиденциальности персональных данных в правилах внутреннего трудового распорядка, положениях о структурных подразделениях Учреждения, должностных инструкциях ов (служащих) и трудовых договорах;

г) порядок передачи персональных данных органам государственной власти, местного самоуправления и сторонним организациям (контрагентам);

д) действенность принимаемых мер по защите охраняемых сведений в ходе подготовки материалов к открытому опубликованию и при изготовлении рекламной продукции;

е) состояние конфиденциального делопроизводства, соблюдение установленного порядка подготовки, учёта, использования, хранения и уничтожения документов, содержащих персональные данные;

ж) выполнение требований по правильному оборудованию защищаемых помещений и предотвращению утечки охраняемых сведений при проведении

мероприятий конфиденциального характера;

з) соответствие защищаемых помещений их техническим паспортам.

Более подробно вопросы, подлежащие проверке, могут раскрываться в отдельных документах (методических рекомендациях, технологических картах, памятках и т.п.).

Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков .

Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

4. Оформление результатов проверки

Результаты проверки оформляются:

1) актом - при проведении проверки комиссией;

2) служебной запиской - при проведении проверки назначенными специалистами.

Акт и/или служебная записка составляется в двух экземплярах и подписывается членами комиссии.

Один экземпляр хранится у ответственного за организацию обработки персональных данных Учреждения. Второй экземпляр хранится в Учреждении в установленном порядке. Копия акта о проверке остается в проверяемом структурном подразделении.

Результаты проверок структурных подразделений периодически обобщаются ответственным за организацию обработки персональных данных в Учреждении и доводятся до руководителей структурных подразделений. При необходимости принятия решений по результатам проверок структурных подразделений на имя Заведующего Учреждения готовятся соответствующие служебные записки.

Заведующий
МБДОУ ДС № 16 «Петушок»



Л.В. Ткаченко

МБДОУ ДС № 16 «Петушок» с. Агой

УТВЕРЖДАЮ

Заведующий

МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко

11 января 2021 года



ПЛАН

внутренних проверок состояния защиты персональных данных

МБДОУ ДС № 16 «Петушок» с. Агой на 2021 год

№ п/п	Наименование структурного подразделения	Месяц											
		Январь	Февраль	Март	Апрель	Май	Июнь	Июль	Август	Сентябрь	Октябрь	Ноябрь	Декабрь
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	Административный персонал												
2	Педагогический персонал												



Заведующий

Л.В. Ткаченко

УТВЕРЖДАЮ



Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко

"11" января 2021 года

АКТ

установления уровня защищенности персональных данных при их обработке в информационной системе МБДОУ ДС 16 "Петушок" с. Агой

Состав комиссии:

Председатель комиссии:

Заведующий Л.В. Ткаченко

Члены комиссии:

Заведующий Л.В. Ткаченко

Старший воспитатель С.Н. Остроухова
председатель профсоюзного комитета Д.С. Куадже
Старшая медицинская сестра Н.В. Бабаян

Комиссия, рассмотрев следующие исходные данные:

1. Информационная система является информационной системой: ИСПДн-С, обрабатывающей специальные категории персональных данных;

2. Информационная система является информационной системой, обрабатывающей персональные данные сотрудников МБДОУ ДС № 16 «Петушок» с. Агой;

3. Информационная система обрабатывает персональные данные менее чем 100 000 субъектов персональных данных;

4. Для информационной системы актуальны угрозы третьего типа. решила установить информационной системе МБДОУ ДС № 16 "Петушок" с. Агой необходимость обеспечения 3 уровня защищенности персональных данных.

Настоящий акт составлен в единственном экземпляре.

Председатель комиссии:

Л.В. Ткаченко

Члены комиссии:

Л.В. Ткаченко

С.Н. Остроухова

Куадже

Д.С. Куадже

Н.В. Бабаян

УТВЕРЖДАЮ

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко
Л.В. Ткаченко

20 *11* года

ПЕРЕЧЕНЬ

**должностей служащих МБДОУ ДС № 16 «Петушок» с. Агой,
ответственных за проведение мероприятий по обезличиванию
обрабатываемых персональных данных**

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1	МБДОУ ДС № 16 "Петушок" с. Агой	Заведующий

Заведующий



Л.В. Ткаченко

УТВЕРЖДАЮ

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

"11" января 2021 года

ПЕРЕЧЕНЬ

лиц МБДОУ ДС № 16 «Петушок» с. Агой имеющих доступ и осуществляющих обработку персональных данных в информационной системе

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1	Медицинский	Медицинская сестра
2	Административный	Заведующий
3	Педагогический	Учитель-логопед, старший воспитатель

Заведующий

Л.В. Ткаченко

Заведующему
МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко

Ф.И.О. субъекта персональных данных

Номер основного документа, удостоверяющего личность

Наименование выдавшего органа

Дата выдачи

ЗАЯВЛЕНИЕ

Прошу Вас прекратить обработку моих персональных данных в связи с

(указать причину)

" ____ " _____ 20 ____ года

(подпись)

(расшифровка подписи)

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН

ПРИКАЗ

11.01. 2021 г.

№ 26/2 - О

с. Агой

Об утверждении перечня лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ

В целях выполнения требований по реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденными приказом ФСБ России 10 июля 2014 года № 378 п р и к а з ы в а ю:


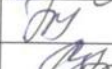




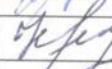
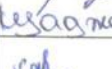


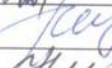
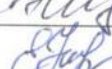



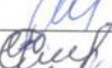
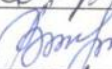
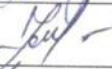
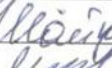






1. Утвердить перечень лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ в соответствии с приложением №1.
2. Приказ довести до всех заинтересованных лиц.
3. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий



Л.В. Ткаченко

Лист ознакомления служащих муниципального бюджетного дошкольного образовательного учреждения детского сада № 16 «Петушок» с. Агой муниципального образования Туапсинский район с положениями законодательства Российской Федерации о персональных данных, с требованиями к защите персональных данных, локальными актами по вопросам обработки персональных данных
«11» января 2021 года

№ п/п	ФИО	Должность	Дата	подпись
1.	Алиева Жанна Васильевна	воспитатель	11.01.2021	
2.	Бабаян Наталия Владимировна	младший воспитатель	11.01.2021	
3.	Брук Виктор Викторович	дворник	11.01.2021	
4.	Губарева Ольга Анатольевна	младший воспитатель	11.01.2021	
5.	Еркин Андрей Валерьевич	Рабочий по ремонту и комплексному обслуживанию зданий	11.01.2021	
6.	Каштанова Елена Вячеславовна	младший воспитатель	11.01.2021	
7.	Крикун Татьяна Николаевна	воспитатель	11.01.2021	
8.	Куадже Диана Сергеевна	воспитатель	11.01.2021	
9.	Кутателадзе Вераника Юрьевна	младший воспитатель	11.01.2021	
10.	Лысенко Светлана Владимировна	повар	11.01.2021	
11.	Мамченко Нина Илинична	кухонный рабочий	11.01.2021	
12.	Мясоедова Ольга Георгиевна	воспитатель	11.01.2021	
13.	Никитенко Вера Васильевна	воспитатель	11.01.2021	
14.	Николаевская Елена Владимировна	воспитатель	11.01.2021	
15.	Новикова Татьяна Ивановна	машинист по стирке и ремонту спецодежды	11.01.2021	
16.	Ноздрина Ирина Викторовна	воспитатель	11.01.2021	
17.	Остроухова Сюзанна Николаевна	старший воспитатель	11.01.2021	
18.	Пирогова Ольга Викторовна	заведующий хозяйством	11.01.2021	
19.	Сусь Ирина Анатольевна	младший воспитатель	11.01.2021	
20.	Хресохоиди Татьяна Викторовна	повар	11.01.2021	
21.	Чакириди Мария Еффалиусовна	младший воспитатель	11.01.2021	
22.	Шайкова Валентина Юрьевна	воспитатель	11.01.2021	
23.	Шурыгина Наталья Николаевна	воспитатель	11.01.2021	
24.	Шхалахова Наталья Карабетовна	младший воспитатель	11.01.2021	
25.	Юрьева Тамара Викторовна	музыкальный руководитель	11.01.2021	

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД
№16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН**

ПРИКАЗ

11.01.2021

№ 26/9 - О

с. Агой

О ведении журнала ознакомления работников МБДОУ ДС
№16 "Петушок" с. Агой, непосредственно осуществляющих обработку
персональных данных, с положениями законодательства Российской
Федерации о персональных данных, в том числе требованиями к защите
персональных данных, документами, определяющими политику оператора в
отношении обработки персональных данных, локальными актами по вопросам
обработки персональных данных и обучения указанных работников

В соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ "О персональных данных", в целях обеспечения требуемого режима безопасности персональных данных МБДОУ ДС №16 "Петушок" с. Агой **п р и к а з ы в а ю**:

1. Ответственному за организацию обработки персональных данных МБДОУ ДС №16 "Петушок" с. Агой организовать проведение первичного инструктажа по вопросам обработки персональных данных со всеми работниками МБДОУ ДС №16 "Петушок" с. Агой, непосредственно осуществляющими обработку персональных данных, до 18.01.2021года.

2. Ответственному за организацию обработки персональных данных МБДОУ ДС №16 "Петушок" с. Агой организовать проведение первичного инструктажа по вопросам обработки персональных данных со всеми принимаемыми на работу работниками, в должностные обязанности которых будет входить обработка персональных данных.

3. Ответственному за организацию обработки персональных данных МБДОУ ДС №16 "Петушок" с. Агой организовывать проведение внепланового инструктажа (или обучения) по вопросам обработки персональных данных с работниками МБДОУ ДС №16 "Петушок" с. Агой, непосредственно осуществляющими обработку персональных данных, при значительных изменениях законодательства Российской Федерации, регулирующего сферу взаимоотношений, возникающих при обработке персональных данных, в том числе требований к защите персональных данных, документов, определяющих политику МБДОУ ДС №16 "Петушок" с. Агой в отношении обработки персональных данных, локальных актов. Решение о необходимости внепланового инструктажа принимает ответственный за организацию

обработки персональных данных МБДОУ ДС №16 "Петушок" с. Агой в каждом отдельном случае.

4. Утвердить форму журнала ознакомления работников с положениями законодательства Российской Федерации о персональных данных, указанную в приложении (далее – Журнал).

5. При проведении инструктажей (обучения) работников по вопросам обработки персональных данных, у проводящему инструктаж или организующему обучение вносить в журнал следующую информацию:

- 1) фамилия, имя, отчество инструктируемого;
- 2) структурное подразделение, должность инструктируемого;
- 3) вид инструктажа;
- 4) дата инструктажа;
- 5) фамилия, имя, отчество инструктирующего;
- 6) структурное подразделение, должность инструктирующего или организующего обучение;
- 7) отметка о проведении инструктажа.

у, проходящему инструктаж (обучение), оставить в журнале отметку о прохождении данного инструктажа (обучения).

6. Контроль ведения журнала возложить на старшего воспитателя Остроухову Сюзанну Николаевну .

7. Назначить ответственным за хранение журнала старшего воспитателя Остроухову Сюзанну Николаевну.

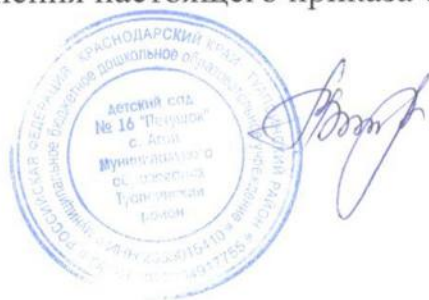
8. Хранение журнала осуществлять в местах, исключающих доступ к журналу посторонних лиц.

9. Хранить журнал в течение 5 лет после завершения ведения.

10. Не допускать копирование персональных данных, указанных в журнале.

11. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий



Л.В. Ткаченко

С приказом ознакомлена:

С.Н. Остроухова

ПРИЛОЖЕНИЕ №1

УТВЕРЖДЕН



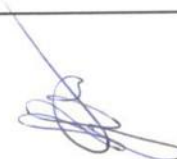

приказом МБДОУ ДС №16 "Петушок"




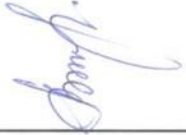






с. Агой от "11"



август 2021 года № 26/9-О

ЖУРНАЛ

ознакомления работников МБДОУ ДС №16 "Петушок" с. Агой, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и обучения указанных работников

№ п/п	ФИО инструктируемого	Структурное подразделение, должность инструктируемого	Вид инструктажа	Дата	ФИО инструктирующего или организацию обучения	Структурное подразделение, должность инструктирующего или организацию обучения	Подпись инструктирующего или организацию обучения	Подпись инструктируемого
1	2	3	4	5	6	7	8	9
1	Пирогова Ольга Викторовна	Административный, заведующий хозяйством	Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением Правительства РФ от 15.09.2008 года № 687)	15.01.2021	Остроухова Сюзанна Николаевна	Педагогический персонал, старший воспитатель		
2	Бабаян Наталия Владимировна	Медицинский, медицинская сестра	Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением	15.01.2021	Остроухова Сюзанна Николаевна	Педагогический персонал, старший воспитатель		

3	Куалже Диана Сергеевна	Председатель ПК, воспитатель	Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением Правительства РФ от 15.09.2008года № 687)	15.01.2021	Остроухова Сюзанна Николаевна	Педагогический персонал, старший воспитатель		
4	Ткаченко Людмила Васильевна	Заведующий	Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. Постановлением Правительства РФ от 15.09.2008года № 687)	15.01.2021	Остроухова Сюзанна Николаевна	Педагогический персонал, старший воспитатель		
1	Пирогова Ольга Викторовна	Административный, заведующий хозяйством	Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных (утв. постановлением Правительства РФ от 6 июля 2008 № 512)	15.01.2021	Остроухова Сюзанна Николаевна	Педагогический персонал, старший воспитатель		
2	Бабаян Наталия Владимировна	Медицинский, медицинская сестра	Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных (утв. постановлением Правительства РФ от 6 июля 2008 № 512)	15.01.2021	Остроухова Сюзанна Николаевна	Педагогический персонал, старший воспитатель		
3	Куалже Диана	Председатель ПК, воспитатель	Требования к материальным носителям биометрических	15.01.2021	Остроухова Сюзанна Николаевна	Педагогический персонал, старший воспитатель		

	Сергеевна			персональных данных и технологий хранения таких данных вне информационных систем персональных данных (утв. постановлением Правительства РФ от 6 июля 2008 № 512									
4	Ткаченко Людмила Васильевна	Заведующий	Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных (утв. постановлением Правительства РФ от 6 июля 2008 № 512	15.01.2021	Остроухова Сюзанна Николаевна	Педагогический персонал, старший воспитатель							

УТВЕРЖДАЮ



Заведующий
МБДОУ ДС №16 «Ягодка» с. Агой

Л.В. Ткаченко

"11" января 2021 года

ПОРЯДОК

доступа служащих МБДОУ ДС № 16 «Петушок» с. Агой в помещения, в которых ведётся обработка персональных данных

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а также обеспечения внутриобъектового режима.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нестандартных ситуациях.

Объектами охраны МБДОУ ДС № 16 «Петушок» с. Агой (далее – Учреждение) являются:

- 1) помещения, в которых происходит обработка персональных данных как с использованием средств автоматизации, так и без таковых, в том числе серверные помещения;
- 2) помещения, в которых хранятся материальные носители персональных данных и резервные копии персональных данных;
- 3) помещения, в которых установлены криптографические средства, предназначенные для шифрования персональных данных, в том числе носители ключевой информации (далее спецпомещения).

Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются и Учреждения, не допущенные к обработке персональных данных и лица, не являющиеся работниками Учреждения.

К спецпомещениям, предъявляются дополнительные требования по безопасности, указанные в разделе 4.

Ответственность за соблюдение положений настоящего порядка несут и структурных подразделений, допущенные в помещения, являющиеся объектами охраны, а также их руководители.

Контроль соблюдения требований настоящей инструкции обеспечивает, назначенный ответственным за организацию обработки персональных данных в Учреждении.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

Например: металлические решётки на окнах, металлическая дверь, система контроля и управления доступа и так далее.

2. Правила доступа в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведётся обработка персональных данных, а также хранятся материальные носители персональных данных и резервные копии персональных данных, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица, из числа работников, допущенных к обработке персональных данных.

При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с

персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведется обработка персональных данных лиц из числа работников Учреждения, не допущенных к обработке персональных данных.

В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка персональных данных, должны быть надежно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

Доступ работников в помещения, в которых ведется обработка персональных данных в нерабочее время, допускается по распоряжению руководства Учреждения.

3. Правила доступа в серверные помещения

Доступ в серверные помещения, в которых ведётся обработка персональных данных осуществляется в соответствии со списком, утверждённым в Учреждении.

Уборка серверных помещений происходит только под контролем лица, из указанных в утверждённом списке.

Доступ в серверные помещения посторонних лиц допускается по согласованию с ответственным за обеспечение безопасности информационных систем персональных.

Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем персональных.

Доступ в серверные помещения в нерабочее время допускается по распоряжению руководства Учреждения.

4. Правила доступа в спецпомещения

Спецпомещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также опечатывание спецпомещений по окончании рабочего дня или оборудование спецпомещений соответствующими техническими устройствами,

сигнализирующими о несанкционированном вскрытии спецпомещений.

Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, утвержденным приказом Заведующего Учреждения.

Доступ иных лиц в спец помещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц их числа работников Учреждения.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Учреждения.

При утрате ключа от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

Доступ работников в спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов), подписанных Заведующим Учреждения.

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко

У Т В Е Р Ж Д А Ю

Заведующий

МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко

11 января 2021 года

П Р А В И Л А

обработки персональных данных в МБДОУ ДС № 16 «Петушок» с. Агой

1. Основные понятия

В настоящем документе используются следующие основные понятия:

автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных – состояние защищённости персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке;

блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных – совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических 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;

несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному назначению и техническим характеристикам;

обработка персональных данных – любое действие (операция) или совокупность действий, 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 (в том числе распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение 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;

персональные данные – любая информация, относящаяся прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных);

предоставление персональных данных – действия, направленные на раскрытие персональных данных определённому лицу или определённому кругу лиц;

распространение персональных данных – действия, направленные на раскрытие

персональных данных неопределённому кругу лиц;

технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных;

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

2. Общие положения

Настоящие правила разработаны для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных МБДОУ ДС № 16 «Петушок» с. Агой (далее – Учреждение), а также защиты прав и свобод граждан при обработке их персональных данных в Учреждении, в том числе право на неприкосновенность частной жизни, личную и семейную тайну, а также разъяснение ответственности должностных лиц (служащих), имеющих доступ к персональным данным, за невыполнение требований норм и правил, регулирующих обработку и защиту персональных данных.

Настоящие правила устанавливают порядок обработки персональных данных субъектов персональных данных в Учреждении и направлены на выявление, предотвращение и профилактику нарушений законодательства Российской Федерации в сфере персональных данных.

Субъектами персональных данных в Учреждении являются:

- 1) граждане, обратившиеся за получением услуги.

Настоящие правила определяют необходимый минимальный объём мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

Настоящие правила разработаны в соответствии со следующими нормативно-правовыми актами Российской Федерации:

- 1) Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года с поправками, одобренными Комитетом министров Совета Европы 15 июня 1999 года, ратифицированная Федеральным законом Российской Федерации от 19 декабря 2005 года № 160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных" в рамках, определяемых данным Федеральным законом, заявлений;

- 2) Конституция Российской Федерации;

- 3) Гражданский кодекс Российской Федерации;

- 4) Кодекс об Административных Правонарушениях Российской Федерации;
- 5) Трудовой кодекс Российской Федерации;
- 6) Уголовный кодекс Российской Федерации;
- 7) Федеральный закон от 27 июля 2004 года № 79-ФЗ "О государственной гражданской службе Российской Федерации";
- 8) Федеральный закон от 27 июля 2006 года № 152-ФЗ "О персональных данных" (далее – Федеральный закон № 152-ФЗ);
- 9) Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- 10) Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 6 марта 1997 года № 188;
- 11) Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждённое постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687;
- 12) Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утверждённый постановлением Правительства Российской Федерации от 21 марта 2012 года № 211;
- 13) Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119.

В соответствии с законодательством Российской Федерации об обработке и защите персональных данных персональные данные субъектов являются конфиденциальной информацией.

В случаях, предусмотренных действующим законодательством, сведения о доходах, об имуществе и обязательствах имущественного характера гражданского служащего, его супруги (супруга) и несовершеннолетних детей могут размещаться на официальном сайте Учреждения или предоставляться региональным средствам массовой информации по их запросам для последующего опубликования.

Порядок регистрации, учёта, оформления, тиражирования, хранения, использования и уничтожения документов и других материальных носителей персональных данных определяют законодательство Российской Федерации об обработке и защите персональных данных, а также действующие нормативные правовые акты Учреждения.

Учреждение является оператором персональных данных субъектов, указанных в настоящем документе. На основании соглашения (договора) Учреждение может поручать обработку персональных данных третьим лицам, с согласия субъекта персональных данных, а в случае если иное предусмотрено действующим законодательством Российской Федерации, то и без их согласия. Существенным условием соглашения (договора) по обработке персональных данных является обязанность обеспечения этими лицами конфиденциальности и безопасности персональных данных субъектов.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со статьёй 24 Конституции Российской Федерации, Учреждение вправе получать и обрабатывать данные о частной жизни гражданских служащих и(или) ов Учреждения только с их письменного согласия.

Учреждение не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством Российской Федерации.

Настоящие Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами обработки персональных данных.

Все изменения в Правила вносятся приказом Заведующего Учреждения.

3. Цель и содержание обработки персональных данных

Целями обработки персональных данных в Учреждении являются:

1) предоставление государственных и муниципальных услуг.

Цель "предоставление государственных и муниципальных услуг" достигается посредством обработки персональных данных следующих категорий для следующих субъектов:

1) граждане, обратившиеся за получением услуги:

Иные категории: фамилия, имя, отчество, контактные сведения, адрес.

4. Правила обработки персональных данных

Все персональные данные субъектов Учреждение получает на законной основе.

Персональные данные ближайших родственников (служащих), необходимые для ведения кадрового учёта, Учреждение получает от самих.

Обработка персональных данных осуществляется в соответствии с действующим законодательством Российской Федерации на основании согласия субъекта персональных данных. Форма согласия утверждается отдельным приказом.

Субъект персональных данных принимает решение о предоставлении своих персональных данных и даёт согласие на их обработку своей волей и в своём интересе.

Учреждение оставляет за собой право не осуществлять свои функции в отношении субъекта персональных данных в случае предоставления неполных или недостоверных персональных данных, а также в случае отказа дать письменное согласие на обработку персональных данных.

При установлении договорных отношений с субъектом персональных данных получение письменного согласия на обработку его персональных данных не требуется.

Получение персональных данных субъекта у третьих лиц возможно только при предварительном уведомлении субъекта и с его письменного согласия. Форма согласия утверждается отдельным приказом.

Персональные данные субъектов Учреждения обрабатываются в структурных подразделениях в соответствии с исполняемыми функциями.

Доступ к персональным данным, обрабатываемым без использования средств автоматизации, осуществляется в соответствии со списком, утверждённым в порядке, определяемом в Учреждении.

Доступ к персональным данным, обрабатываемым в информационных системах персональных данных, осуществляется в соответствии со списком, утверждённым в порядке, определяемом в Учреждении.

Уполномоченные лица, допущенные к персональным данным субъектов Учреждения, имеют право получать только те персональные данные субъекта, которые необходимы для выполнения конкретных функций, в соответствии с должностными инструкциями указанных лиц.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна выполняться в соответствии с требованиями "Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" утверждённого Постановлением Правительства РФ от 15 сентября 2008 № 687.

Персональные данные при такой их обработке, должны обособляться от иной информации, в частности путём фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки.

Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются приказом об утверждении мест хранения материальных носителей персональных данных Учреждения.

Персональные данные подлежат уничтожению либо обезличиванию в случаях достижения целей или в случае утраты необходимости в достижении этих целей, отзыва согласия субъекта персональных данных, выявления неправомерной обработки персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

В срок, не превышающий 7 рабочих дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения, а также уведомляет субъекта о внесённых изменениях.

Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, если иное не предусмотрено федеральным законом Российской Федерации.

Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента отзыва согласия субъекта персональных данных.

Уничтожение персональных данных осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

Уничтожение персональных данных осуществляется в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных. Учреждение уведомляет об этом субъекта или его законного представителя.

Уничтожение персональных данных на бумажных носителях осуществляет комиссия в составе руководителя и работников структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

- 1) сжигание;
- 2) шредирование (измельчение);
- 3) передача на специализированные полигоны (свалки);
- 4) химическая обработка.

При этом составляется "Акт уничтожения документов Учреждения, содержащих персональные данные субъекта". Форма акта утверждается отдельным приказом.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Учреждения должна присутствовать при уничтожении материальных носителей персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, выполняется по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, осуществляет комиссия, в состав которой входят лица, ответственные за администрирование автоматизированных систем, которым принадлежат базы данных, и структурного подразделения, обрабатывавшего персональные данные субъекта и

установившего необходимость их уничтожения.

Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, достигается путём затирания информации на носителях информации (в том числе и резервных копиях) или путём механического нарушения целостности носителя информации, не позволяющего произвести считывание или восстановление персональных данных. При этом составляется "Акт уничтожения полей баз данных Учреждения, содержащих персональные данные субъекта". Форма акта утверждается отдельным приказом.

Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определённого срока предусмотрены соответствующими нормативными и (или) договорными документами.

При невозможности осуществления затирания информации на носителях допускается проведение обезличивания путём перезаписи полей баз данных, которые позволяют определить субъекта, данными, исключая дальнейшее определение субъекта.

Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных в Учреждении.

Обработка биометрических персональных данных (фотография, отпечатки пальцев, сетчатки глаза и другое), в соответствии со статьёй 11 Федерального закона № 152, допускается при наличии согласия субъекта. Форма согласия утверждается отдельным приказом.

Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных.

и (служащие) Учреждения должны быть ознакомлены под роспись с требованиями законодательства Российской Федерации, касающимися обработки персональных данных, настоящими Правилами и другими документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

5. Передача персональных данных третьим лицам

При обработке персональных данных субъекта должны соблюдаться следующие требования:

1) не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта. Форма согласия утверждается отдельным приказом. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащими персональные данные субъекта, при условии соблюдения требований статьи 9 Федерального закона № 152;

2) предупреждать лиц, получающих 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, получающие персональные данные субъекта, обязаны соблюдать режим конфиденциальности в отношении этих данных.

При необходимости трансграничной передачи персональных данных на территорию иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, Учреждение запрашивает согласие субъекта в письменной форме. Форма согласия утверждается отдельным приказом.

6. Права субъектов персональных данных

В целях обеспечения своих интересов субъекты имеют право:

1) получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

2) осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных Федеральным законом;

3) требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона № 152-ФЗ. Субъект персональных данных, при отказе Учреждения исключить или исправить персональные данные субъекта, имеет право заявлять в письменной форме о своём несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера субъект имеет право дополнить заявлением, выражающим его собственную точку зрения;

4) требовать от Учреждения уведомления всех лиц, которым ранее были сообщены неверные или неполные персональные данные субъекта, обо всех произведённых в них изменениях или исключениях из них;

5) обжаловать в суде любые неправомерные действия или бездействие Учреждения при обработке и защите персональных данных субъекта.

7. Порядок действий в случае запросов надзорных органов

В соответствии с частью 4 статьи 20 Федерального закона № 152 Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных в Учреждении при необходимости с привлечением ов (служащих) Учреждения.

В течение установленного законодательством срока ответственный за организацию обработки персональных данных в Учреждении подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

8. Защита персональных данных субъекта

Защиту персональных данных субъектов от неправомерного их использования или утраты Учреждение обеспечивает за счёт собственных средств в порядке, установленном законодательством Российской Федерации.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с:

1) РД ФСТЭК России – "Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных". Утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года;

2) специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утвержденными приказом Гостехкомиссии России от 30 августа 2002 года № 282;

3) внутренними документами Учреждения, действующими в сфере обеспечения информационной безопасности.

Защита персональных данных предусматривает ограничение к ним доступа.

Ответственные за организацию обработки персональных данных, администрирование средств и механизмов защиты, техническое обслуживание информационных систем персональных данных назначаются приказом Заведующего Учреждения.

Руководитель структурного подразделения Учреждения, осуществляющего обработку персональных данных:

- 1) несёт ответственность за организацию защиты персональных данных в структурном подразделении;
 - 2) организует изучение уполномоченными лицами нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;
 - 3) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении (отделе);
 - 4) контролирует порядок доступа к персональным данным в соответствии с функциональными обязанностями сотрудников подразделения.
- и (служащие), допущенные к персональным данным дают письменное обязательство о неразглашении таких данных.

9. Обязанности лиц, допущенных к обработке персональных данных

Лица, допущенные к работе с персональными данными, обязаны:

- 1) знать законодательство Российской Федерации в области обработки и защиты персональных данных, нормативные документы Учреждения по защите персональных данных;
- 2) сохранять конфиденциальность персональных данных;
- 3) обеспечивать сохранность закреплённых за ними носителей персональных данных;
- 4) контролировать срок истечения действия согласий на обработку персональных данных и, при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;
- 5) докладывать своему непосредственному руководителю структурного подразделения обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

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

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, привлекаются к материальной, административной, уголовной и гражданско-правовой ответственности на основании судебного решения, а также к дисциплинарной ответственности в соответствии с действующим законодательством Российской Федерации.

К данным лицам могут быть применены следующие дисциплинарные взыскания:

- 1) замечание;
- 2) выговор;
- 3) предупреждение о неполном должностном соответствии;
- 4) увольнение с гражданской службы.

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко

УТВЕРЖДАЮ

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко

"11" января 2021 года



ПЕРЕЧЕНЬ

**должностей служащих МБДОУ ДС № 16 «Петушок» с. Агой,
ответственных за проведение мероприятий по обезличиванию
обрабатываемых персональных данных**

№ п/п	Структурное подразделение (отдел)	Должность служащего
1	2	3
1	МБДОУ ДС № 16 "Петушок" с. Агой	Заведующий

Заведующий

Л.В. Ткаченко

МБДОУ ДС № 16 «Петушок» с. Агой

УТВЕРЖДАЮ

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой
Л.В. Ткаченко
"11" января 2021 года



ПЛАН

мероприятий по защите персональных данных
в МБДОУ ДС № 16 «Петушок» с. Агой на 2021 г.

№ п/п	Наименование мероприятия	Срок выполнения	Ответственный за выполнение	Примечание
1	2	3	4	5
1	Классификация информационных систем персональных данных (ИСПДн)	3 квартал 2021 года	Комиссия (Председатель: Заведующий Л.В. Ткаченко)	Проводится при создании ИСПДн, при выявлении в информационных системах наличия персональных данных, при изменении состава, структуры самой ИСПДн или технических особенностей ее построения
2	Выявление угроз безопасности персональных данных и разработка моделей угроз и нарушителя	3 квартал 2021 года	Заведующий Л. В. Ткаченко	Разрабатывается после установления уровня защищенности персональных данных в ИСПДн
3	Направление в уполномоченный орган (Роскомнадзор) уведомления о своем намерении осуществлять обработку персональных данных с использованием средств автоматизации	3 квартал 2021 года	Заведующий Л. В. Ткаченко	Уведомление направляется при вводе в эксплуатацию новых ИСПДн, либо при внесении изменений в существующие
4	Проверка сведений, содержащихся в уведомлении	ежеквартально	Заведующий Л. В. Ткаченко	По необходимости, в Роскомнадзор отправляется измененная версия уведомления
5	Документальное регламентирование работы с персональными данными	3 квартал 2021 года	Заведующий Л. В. Ткаченко	Необходимо разработать документы, распределяющие и закрепляющие ответственность за обработку персональных данных
6	Проведение первичного инструктажа по вопросам обработки персональных данных со всеми работниками МБДОУ ДС № 16 «Петушок» с. Агой с осуществлением ознакомления	3 квартал 2021 года	Заведующий Л. В. Ткаченко	Необходимо проводить инструктаж по обработке персональных данных и ознакомить с требованиями законодательства Российской

	работников с положениями законодательства Российской Федерации о персональных данных			Федерации о персональных данных и внутренними локальными актами по защите персональных данных
7	Проведение первичного инструктажа по вопросам обработки персональных данных с принимаемыми на работу в МБДОУ ДС № 16 «Петушок» с. Агой осуществлением ознакомления с положениями законодательства Российской Федерации о персональных данных	Постоянно	Заведующий Л. В. Ткаченко	Необходимо проводить отдельный инструктаж по обработке персональных данных с принимающимися на работами
8	Заключение договора на проведение работ в области защиты персональных данных с организацией – лицензиатом ФСТЭК России	4 квартал 2021 года	Заведующий Л. В. Ткаченко	
9	Оценка соответствия эффективности принимаемых мер по обеспечению безопасности персональных данных в ИСПДн МБДОУ ДС № 16 «Петушок» с. Агой в форме аттестации	4 квартал 2021 года		Проводится организацией – лицензиатом ФСТЭК России
10	Разработка приказа о вводе ИСПДн в эксплуатацию	По завершении мероприятий по оценке соответствия	Заведующий Л. В. Ткаченко	
11	Заключение договора с компанией - лицензиатом ФСТЭК России и ФСБ России на аутсорсинг технической защиты персональных данных	По завершении мероприятий по оценке соответствия	Заведующий Л. В. Ткаченко	При необходимости
12	Пересмотр договоров с субъектами и контрагентами в части обработки персональных данных, получение письменного согласия субъекта на обработку персональных данных	4 квартал 2021 года, в последующем – постоянно, при заключении новых договоров	Заведующий Л. В. Ткаченко	В договоры должны быть включены согласия субъекта на обработку и передачу его персональных данных

13	Уничтожение персональных данных	При достижении целей обработки персональных данных	Комиссия по уничтожению документов	
14	Сопровождение заявок на предоставление доступа к информационным ресурсам ИСПДн	Постоянно	Заведующий Л. В. Ткаченко	
15	Повышение квалификации в области защиты персональных данных		Заведующий Л. В. Ткаченко	и, ответственные за организацию обработки персональных данных и обеспечение безопасности ИСПДн – не реже чем раз в три года. Повышение осведомлённости, обрабатывающих персональные данные – постоянно. Повышение осведомлённости может осуществляться путём проведения инструктажа ответственным за организацию обработки персональных данных либо обучением учебных центрах.

Заведующий



Л.В. Ткаченко

УТВЕРЖДАЮ

Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой



Л.В. Ткаченко
2021 года

ПЕРЕЧЕНЬ
информационных систем персональных данных
МБДОУ ДС № 16 «Петушок» с. Агой

№	Наименование ИСПДн	Категория ИСПДн	Уровень защищенности персональных данных	Использование СКЗИ для обеспечения безопасности персональных данных
1	2	3	4	5
1	МБДОУ ДС 16 Петушок	ИСПДн-С	третий	не используются

Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) "О персональных данных"

Статья 12. Трансграничная передача персональных данных

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

(см. текст в предыдущей редакции)

1. Трансграничная передача персональных данных на территории иностранных государств, являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иных иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, осуществляется в соответствии с настоящим Федеральным законом и может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства.

2. Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, не являющихся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных. Государство, не являющееся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, может быть включено в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер безопасности персональных данных.

3. Оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления трансграничной передачи персональных данных.

4. Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

1) наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;

2) предусмотренных международными договорами Российской Федерации;

3) предусмотренных федеральными законами, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и

государства в сфере транспортного комплекса от актов незаконного вмешательства;

4) исполнения договора, стороной которого является субъект персональных данных;

5) защиты жизни, здоровья, иных жизненно важных интересов субъекта персональных данных или других лиц при невозможности получения согласия в письменной форме субъекта персональных данных.

Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 02.07.2021) "О персональных данных"

Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных

1. Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных частью 2 настоящей статьи.

2. Решение, порождающее юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных данных или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

3. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

4. Оператор обязан рассмотреть возражение, указанное в части 3 настоящей статьи, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

(в ред. Федерального закона от 25.07.2011 N 261-ФЗ)

(см. текст в предыдущей редакции)

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН

ПРИКАЗ

11.01.2021 г.

№ 26/3 - О

с. Агой

Об ответственности за обработку и защиту персональных данных МБДОУ
ДС № 16 «Петушок» с. Агой МО Туапсинский район

В целях обеспечения режима конфиденциальности персональных данных, разграничения прав доступа к информационным системам персональных данных, распределения ответственности за техническое обслуживание объектов информатизации МБДОУ ДС № 16 «Петушок»

с. Агой п р и к а з ы в а ю:

1. Распределить ответственность за обработку и защиту персональных данных в соответствии с перечнем лиц, указанным в приложении № 1.

2. Организовать доступ к персональным данным, обрабатываемым без использования средств автоматизации, в соответствии с перечнем лиц, указанным в приложении № 2.

3. Организовать доступ к персональным данным, обрабатываемым в информационных системах персональных данных, в соответствии с перечнем лиц, указанным в приложении № 3.

4. Приказ довести до всех заинтересованных лиц.

5. Контроль за исполнением настоящего приказа возложить на Ответственного за организацию обработки персональных данных.

Заведующий



Л.В. Ткаченко

ПРИЛОЖЕНИЕ № 1
к приказу МБДОУ ДС № 16
«Петушок» с. Агой
от "11" января 2021 года № 18/3

ПЕРЕЧЕНЬ
лиц, ответственных за защиту и техническое обслуживание
информационных систем персональных данных

№ п/п	Ответственность	Должность	Фамилия, инициалы
1	2	3	4
1	Ответственный за обезличивание персональных данных	Заведующий	Ткаченко Л.В.
2	Ответственный за техническое обслуживание информационных систем персональных данных	Заведующий	Ткаченко Л.В.
3	Ответственный за обеспечение безопасности информационных систем персональных данных - Администратор информационной безопасности	Заведующий	Ткаченко Л.В.

ПРИЛОЖЕНИЕ № 2
к приказу МБДОУ ДС № 16 «Петушок»
с. Агой
от "11" сентября 2021 года № 26/3

ПЕРЕЧЕНЬ

лиц, имеющих право доступа к персональным данным, обрабатываемым
без использования средств автоматизации

№ п/п	Должность, Фамилия и инициалы	Полномочия
1	2	3
Администрация		
1	Заведующий хозяйством .	обработка
Педагогический		
2	Старший воспитатель, учитель - логопед Остроухова С.Н.	обработка

ПРИЛОЖЕНИЕ № 2
к приказу МБДОУ ДС № 16 «Петушок»
с. Агой
от "11" сентября 2021 года № 16/3

ПЕРЕЧЕНЬ

лиц, имеющих право доступа к информационным системам персональных данных МБДОУ ДС № 16 «Петушок» с. Агой

Лица, имеющие право доступа к ИСПДн МБДОУ ДС 16 «Петушок» с. Агой

№ п/п	Должность, Фамилия и инициалы	Полномочия
1	2	3
Администрация		
1	Заведующий хозяйством .Пирогова О.В.	пользователь
Педагогический		
1	Старший воспитатель, учитель - логопед Остроухова С.Н.	полный доступ
Медицинский		
1	медицинская сестра Бабаян Н.В.	полный доступ

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН

ПРИКАЗ

11.01.2021 г.

№ 26/10 - О

с. Агой

О журнале регистрации инцидентов информационной безопасности МБДОУ
ДС №16 "Петушок" с. Агой

В соответствии с требованиями "Положения по работе с инцидентами информационной безопасности" МБДОУ ДС №16 "Петушок" с. Агой, в целях обеспечения требуемого режима информационной безопасности **п р и к а з ы в а ю:**

1. Утвердить форму журнала регистрации инцидентов информационной безопасности, указанную в приложении.

2. Регистрировать в журнале все инциденты информационной безопасности.

3. При выявлении инцидентов информационной безопасности вносить в журнал следующую информацию:

- 1) фамилия, имя, отчество, должность, структурное подразделение работника обнаружившего инцидент;
- 2) дата выявления инцидента;
- 3) описание инцидента;
- 4) принятые меры по устранению последствий инцидента;
- 5) причины возникновения инцидента;
- 6) размер потенциально-возможного ущерба;
- 7) размер фактического ущерба;
- 8) принятые меры по предотвращению повторного возникновения инцидента.

4. Допускается ведение журнала в электронном виде.

5. Назначить ответственным за ведение и сохранность журнала старшего воспитателя Остроухову Сюзанну Николаевну.

6. Хранение журнала осуществлять в местах, исключающих доступ к журналу посторонних лиц.

7. Хранить журнал в течение 5 лет после завершения ведения.

8. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий



Л.В. Ткаченко

Перечень лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ:

1. Ткаченко Людмила Васильевна
2. Остроухова Сюзанна Николаевна
3. Бабаян Наталия Владимировна
4. Куадже Диана Сергеевна
5. Пирогова Ольга Викторовна

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН**

ПРИКАЗ

11.01. 2021 г.

№ 26/7- О

с. Агой

Об утверждении мест хранения материальных носителей персональных данных
МБДОУ ДС № 16 "Петушок" с. Агой

В соответствии с требованиями Положения об особенностях обработки персональных данных субъектов, осуществляемой без использования средств автоматизации, утверждённого постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687, в целях обеспечения режима конфиденциальности при работе с материальными носителями персональных данных в МБДОУ ДС №16 "Петушок" с. Агой (далее – Учреждение) **п р и к а з ы в а ю:**

1. Обеспечить раздельное хранение материальных носителей персональных данных субъектов Учреждения.

2. Соблюдать при хранении материальных носителей персональных данных условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. В нерабочее время помещения, в которых хранятся материальные носители, должны сдаваться под охрану. При этом все окна и двери должны быть надёжно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы).

3. Утвердить перечень мест хранения материальных носителей персональных данных субъектов Учреждения в соответствии с приложением к данному приказу.

4. Хранить материальные носители персональных данных только в установленных местах.

5. Для хранения материальных носителей персональных данных помещения оборудовать сейфами, запираемыми шкафами или шкафами для бумаг с устройством опечатывания.

6. Назначить ответственных лиц за обеспечение сохранности материальных носителей персональных данных в соответствии с приложением к данному приказу.

7. Ознакомить лиц, ответственных за обеспечение сохранности материальных носителей персональных данных, с постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" под подпись.

8. Контроль исполнения настоящего приказа возлагаю на себя. ...

Заведующий



Л.В. Ткаченко

С приказом № 26/8 – О от 11.01.2021 г. ознакомлены, согласны:

Ф.И.О.	Должность	Подпись
Остроухова Сюзанна Николаевна	старший воспитатель	
Бабаян Наталия Владимировна	медицинская сестра	
Куадже Диана Сергеевна	председателя профсоюзного комитета	
Пирогова Ольга Викторовна	заведующий хозяйством	

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН

ПРИКАЗ

11.01. 2021 г.

№ 26/5 - О

с. Агой

Об установлении границ контролируемой зоны объектов информатизации
МБДОУ ДС № 16 «Петушок» с. Агой

В целях исполнения требований Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных" и реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёнными приказом ФСТЭК России от 18 февраля 2013 года № 21 п р и к а з ы в а ю:

Считать границей контролируемой зоны объектов информатизации ограждающие конструкции помещений, в которых располагаются компоненты информационных систем персональных данных МБДОУ ДС № 16 «Петушок» с. Агой.

Заведующий



Л.В. Ткаченко

УТВЕРЖДАЮ



Заведующий
МБДОУ ДС № 16 «Петушок» с. Агой

Л.В. Ткаченко Л.В. Ткаченко

11 января 2021 года

ПЕРЕЧЕНЬ МЕР, ПРЕПЯТСТВУЮЩИХ НЕСАНКЦИОНИРОВАННОМУ ДОСТУПУ К ПЕРСОНАЛЬНЫМ ДАННЫМ

І. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий Перечень мер, направленных на предотвращение неправомерного использования персональных данных (далее - Перечень мер) муниципального бюджетного дошкольного образовательного учреждения детского сада № 16 «Петушок» с. Агой (далее - ДОУ) определяет порядок противодействия несанкционированному использованию персональных данных сотрудниками, имеющими доступ к такой информации, а также их ответственность, в случае совершения ими действий, повлекших неправомерное использование персональных данных.

Целью настоящего документа является установление в учреждении процедур, позволяющих:

исключить возможность несанкционированного доступа к персональным данным их использования работниками учреждения и третьими лицами в собственных интересах в ущерб интересам граждан;

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Перечне мер применяются следующие термины и определения:

Персональные данные (ПД) - любая информация, относящаяся к определенному или определяемому на основании такой информации и физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или)осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

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 наличия таких средств.

1.1.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.

1.2. Применяемые в Перечне мер понятия и определения, не приведенные в настоящем разделе, используются в соответствии с понятиями и определениями, содержащимися в законодательстве Российской Федерации.

II. ОБЩИЕ ПОЛОЖЕНИЕ О ПЕРСОНАЛЬНЫХ ДАННЫХ И ПОРЯДКЕ ИХ ИСПОЛЬЗОВАНИЯ

2.1. Персональные данные могут быть представлены в различном виде, в том числе в бумажном или электронном.

2.2. Персональные данные могут передаваться только тем лицам, которым они необходимы для исполнения ими своих прямых должностных обязанностей.

2.3. Сотрудники ДООУ, осуществляющие проведение, обработку и учет персональных данных не имеют права передавать данную информацию третьим лицам и работникам ДООУ, режим доступа которых не предусматривает возможности обладания такой информацией, либо использовать ее в личных целях.

2.4. За использование и разглашение персональных данных, сотрудник ДООУ несет персональную ответственность в соответствии с должностной инструкцией и действующим законодательством РФ.

III. ОСНОВНЫЕ МЕРЫ (ПРОЦЕДУРЫ), ПРЕПЯТСТВУЮЩИЕ НЕСАНКЦИОНИРОВАННОМУ ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Под процедурами, препятствующими несанкционированному использованию персональных данных, в целях реализации настоящего документа, понимаются мероприятия по предупреждению несанкционированного использования, оперативному и последующему контролю использования персональных данных, проводимые сотрудниками ДООУ.

3.2. В ДООУ применяются следующие меры, препятствующие несанкционированному доступу к персональным данным:

- ограничение доступа к персональным данным в специализированных программных средствах;

- защита персональных данных при их обработке и архивировании;

- ограничение доступа посторонних лиц в помещения учреждения, предназначенные для осуществления работы с ПД;

- защита рабочих мест работников, осуществляющих операции с программными средствами;

- контроль за соблюдением работниками ДООУ требований законодательства РФ и иных нормативных правовых актов.

3.3. В целях противодействия несанкционированному использованию персональных данных, предотвращения утечки и обеспечения сохранности персональных данных, ДООУ используется комплекс мероприятий.

3.4. Ограничение доступа к служебной информации в программных средствах:
- обеспечение доступа к данным только в пределах полномочий, обработку и учет информации с ПД;

- установление индивидуальных кодов и паролей доступа к данным для каждого исполнителя;
- осуществление административных и технических мер, направленных на исключение несанкционированного доступа к данным: блокирование доступа пользователя в систему, в случае обнаружения попыток несанкционированного доступа, установка программных средств, оповещающих ответственного за организацию работы по обеспечению защиты информации о попытке несанкционированного доступа, блокировка рабочего места нарушителя;
- контроль за соблюдением режима обращения персональных данных осуществляется ответственным за организацию работы по обеспечению защиты информации, а также заведующим ДОУ.

3.5. Защита персональных данных при ее обработке и архивировании:

- обеспечение дублирования данных в процессе их ввода, предусматривающее сохранность первичного носителя информации;
- установка программных средств для создания резервных копии, способствующих быстрому восстановлению данных;
- использование систем защиты информационно-технических систем и каналов связи от утечки персональных данных;
- осуществление резервного копирования (восстановления) только уполномоченными сотрудниками.

3.6. Ограничение доступа посторонних лиц в помещении ДОУ, предназначенные для осуществления сбора, обработки и хранения информации ПД осуществляются за счёт.

- 3.7. Соблюдения порядка и правил доступа в служебные помещения в соответствии с Положением о защите ПД в ДОУ, утвержденном заведующим;
- ограничением доступа работников и посторонних лиц в помещение, в котором размещены персональные компьютеры, вычислительные системы и системы телекоммуникации для осуществления операций с ПД.

3.8. Защита рабочих мест работников, осуществляющих сбор и обработку ПД:

- защита окон в служебных помещениях от внешне дистанционного наблюдения жалюзи и шторами;
- эффективное размещение рабочих мест сотрудников для исключения возможности несанкционированного просмотра документов и информации на мониторах;
- соблюдение сотрудниками подразделений правил по обеспечению защиты информации при работе с персональными компьютерами.

3.9. Ограничение доступа к персональным данным:

- доступ работников к необходимым документам, только для
- выполнения своих служебных обязанностей;
- проведение инвентаризации мест хранения документов, содержащих персональные данные;
- контроль за соблюдением утвержденных внутренних регламентов.

3.10. При оформлении на работу в ДОУ, работник дает расписку о неразглашении персональных данных.

3.11. Контроль за соблюдением работниками ДОУ требований законодательства РФ и иных нормативных правовых актов, регулирующих работу с ПД, внутренними документами, возложена на заведующего ДОУ.

IV. ОСУЩЕСТВЛЕНИЕ ПРОЦЕДУР, ПРЕПЯТСТВУЮЩИХ НЕСАНКЦИОНИРОВАННОМУ ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ, И КОНТРОЛЯ ЗА ИХ ИСПОЛНЕНИЕМ

- 4.1. Проведение процедур, препятствующих несанкционированному использованию персональных данных и осуществление контроля включают в себя:
- 4.2. Установление требований о неразглашении персональных данных.
- 4.3. Контроль за выполнением работниками ДООУ требований действующего законодательства РФ и внутренних документов ДООУ.
- 4.4. Уведомление работников ДООУ, имеющих доступ к информации о ПД, о недопустимости осуществления операций с ПД как в своих интересах, так и в интересах третьих лиц.
- 4.5. Проведение оперативных проверок на предмет возможной утечки персональных данных в случаях, предполагающих несанкционированное использование персональных данных.
- 4.6. Направление сведений руководству ДООУ об установленных (обнаруженных) случаях несанкционированного использования персональных данных.

V. ОТВЕТСТВЕННОСТЬ

5.1 Ответственный за организацию работы по обеспечению защиты информации отвечает за:

- осуществление контроля исполнения положений нормативных документов по вопросам организации эффективного функционирования системы внутреннего контроля ДООУ;
- контроль исполнения внутренних нормативных документов учреждения по вопросам обеспечения конфиденциальности персональных данных в ДООУ;
- проведение служебных расследований по фактам возможного неправомерного использования работниками ДООУ персональных данных, о результатах которых незамедлительно уведомляет заведующего.

5.2. Работники ДООУ, которым стали известны факты неправомерного использования персональных данных при осуществлении профессиональной деятельности, должны незамедлительно доложить об этом заведующему ДООУ.

5.3. Ответственность сотрудников и должностных лиц ДООУ за нарушения режима обращения с персональными данными и порядок наложения взыскания:

5.4. Виды взысканий, применяемых к сотрудникам и должностным лицам ДООУ нарушившим режим обращения с персональными данными:

- предупреждение;
- выговор;
- увольнение с работы;

5.5. Взыскание на сотрудника ДООУ налагается заведующим.

VI. МЕСТА РАЗДЕЛЬНОГО ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Для исключения несанкционированного доступа к ПД в ДОУ приказом заведующего определяются места раздельного хранения персональных данных (материальных носителей) в отношении каждой категории персональных данных и устанавливается перечень лиц, осуществляющих обработку персональных данных.

Место хранения ПД	Наименование документов, содержащих ПД	Должность сотрудника, ответственного за хранение ПД
Кабинет заведующего Шкаф Сейф	Информация о сотрудниках и обучающихся на электронных носителях Трудовые сотрудников ДОУ Личные дела, личные карточки Т-2, Приказы по личному составу	Заведующий
Сейф в кабинете заведующего	Личные дела обучающихся, Книга учета воспитанников	Заведующий Делопроизводитель
Шкаф в кабинете заведующего	Личные дела детей	Заведующий
Кабинет заведующего Шкаф Сейф	Тарификация, Табель на зарплату. Расчетные листки. Лицевые счета. Больничные листки. Приказы по личному составу	Заведующий
Медицинский кабинет	Медицинские карты обучающихся и мед книжки сотрудников	Медицинский работник

6.2. Ответственный за организацию работы по обеспечению защиты информации осуществляет ознакомление сотрудников ДОУ с настоящим Перечнем мер не позднее одного месяца со дня его вступления в силу. Факт ознакомления подтверждается подписью сотрудника. В дальнейшем, проводится регулярный инструктаж сотрудников с периодичностью не реже одного раза в год, с целью неукоснительного соблюдения сотрудниками мероприятий, направленных на предотвращение неправомерного использования персональных данных при осуществлении учреждения профессиональной деятельности.

6.3. Ответственный за организацию работы по обеспечению защиты информации, в случае принятия в штат ДОУ нового сотрудника, осуществляет ознакомление с настоящим Перечнем мер не позднее одной недели со дня его зачисления в штат.

6.4. Работники ДОУ должны предпринимать все необходимые меры,

позволяющие предотвратить неправомерное распространение и использование персональных данных при проведении операции, связанных с осуществлением профессиональных видов деятельности.

Заведующий
МБДОУ ДС №16 «Петушок» с. Агой



Л.В. Ткаченко

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН

ПРИКАЗ

11.01.2021 г.

№ 26/4 - О

с. Агой

Об утверждении форм актов уничтожения персональных данных

В целях исполнения требований Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных", приказываю:

1. Утвердить форму акта уничтожения документов, содержащих персональные данные субъекта, указанную в приложении № 1.

2. Утвердить форму акта уничтожения полей баз данных, содержащих персональные данные субъекта, указанную в приложении № 2.

3. В порядке, установленном в МБДОУ ДС № 16 «Петушок» с. Агой, осуществлять уничтожение персональных данных, используя формы актов уничтожения, указанные в приложениях к данному приказу.

4. В случаях, если уничтожение персональных данных осуществляется после обращения или письменного запроса субъекта персональных данных, ответственному за организацию обработки персональных данных МБДОУ ДС № 16 «Петушок» с. Агой обеспечить направление субъекту персональных данных уведомления об уничтожении персональных данных, указанного в приложении № 3.

5. Приказ вступает в силу со дня его подписания.

6. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий



Л.В. Ткаченко

ПРИЛОЖЕНИЕ № 1

УТВЕРЖДЕН
приказом МБДОУ ДС № 16
«Петушок» с. Агой
от "11" января 2021 года № 26/4

А К Т № _____
уничтожения документов МБДОУ ДС № 16 «Петушок» с. Агой,
содержащих персональные данные субъекта

Состав комиссии:

Председатель комиссии:

Члены комиссии:

Комиссия произвела отбор к уничтожению следующих документов, содержащих персональные данные субъекта персональных данных:

№ п/п	Наименование документа	Регистрационный номер документа	Дата регистрации	Номер экз.	Количество листов документа /приложения
1	2	3	4	5	6

Причина уничтожения:

- достижение целей обработки персональных данных решение субъекта персональных данных недостоверные персональные данные

Всего подлежит уничтожению _____ (цифрами) _____ (прописью)

наименований документов.

Документы уничтожены с помощью _____

(указать способ уничтожения)

Председатель комиссии:

Члены комиссии:

ПРИЛОЖЕНИЕ № 2

УТВЕРЖДЕН
приказом МБДОУ ДС № 16
«Петушок» с. Агой
от "11" января 2021 года № 26/4

А К Т № _____
уничтожения полей баз данных МБДОУ ДС № 16 «Петушок» с. Агой,
содержащих персональные данные субъекта

Состав комиссии:

Председатель комиссии:

Члены комиссии:

Комиссия произвела отбор к уничтожению следующих полей баз данных, содержащих персональные данные субъекта персональных данных:

№ п/п	Наименование базы данных	Идентификационный номер поля данных	Наименование полей данных
1	2	3	4

Причина уничтожения:

- достижение целей обработки персональных данных решение субъекта персональных данных недостоверные персональные данные

Всего подлежит уничтожению _____ (цифрами) _____ (прописью)

наименований полей базы данных.

Поля баз данных уничтожены путем затирания информации на носителях информации (в том числе и резервных копиях).

Председатель комиссии:

Члены комиссии:

ПРИЛОЖЕНИЕ № 3
УТВЕРЖДЕН
приказом МБДОУ ДС № 16
«Петушок» с. Агой
от "11"

сентябрь 2021 года № *26/4*

**УВЕДОМЛЕНИЕ
об уничтожении персональных данных**

Уважаемый _____
Ф.И.О. субъекта персональных данных

Обработка Ваших персональных данных прекращена.
Ваши персональные данные, которые обрабатывались в МБДОУ ДС № 16 «Петушок» с. Агой, были уничтожены.

Приложение: копия акта об уничтожении на _____ листах.

Ответственный за организацию
обработки персональных данных
МБДОУ ДС № 16 «Петушок» с. Агой

Заведующий



Л.В. Ткаченко

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД №16 «ПЕТУШОК» С. АГОЙ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
ТУАПСИНСКИЙ РАЙОН

ПРИКАЗ

11.01.2021 г.

№ 26/8 - О

с. Агой

О допуске пользователей к работе с криптографическими
средствами защиты информации

Во исполнение требований приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) от 13 июня 2001 года № 152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" при работе с криптографическими средствами защиты информации "Петушка" п р и к а з ы в а ю:

1. Утвердить перечень лиц, допущенных к работе с шифровальными (криптографическими) средствами в соответствии с приложением № 1).

2. Допустить к работе с криптографическим средствам защиты информации лиц, указанных в приложении № 1.

3. Ответственность за функционирование и безопасность криптографических средств защиты информации возложить на ответственного пользователя СКЗИ.

Приложение: 1. Перечень лиц, допущенных к работе с шифровальными (криптографическими) средствами.

Заведующий



Л.В. Ткаченко

**Перечень лиц, допущенных к работе с шифровальными
(криптографическими) средствами**

№ п/п	Должность	Фамилия, инициалы	Помещение	Наименование криптосредства
1.	заведующий	Ткаченко Л.В.	Кабинет заведующего	VipNet Client 3.2

**Постановление Правительства РФ от 6 июля 2008 г. N 512
"Об утверждении требований к материальным носителям
биометрических персональных данных и технологиям
хранения таких данных вне информационных систем
персональных данных" (с изменениями и дополнениями)**

**Постановление Правительства РФ от 6 июля 2008 г. N 512
"Об утверждении требований к материальным носителям
биометрических персональных данных и технологиям хранения
таких данных вне информационных систем персональных данных"
С изменениями и дополнениями от:**

27 декабря 2012 г.

Правительство Российской Федерации постановляет:

1. Утвердить прилагаемые требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.
2. Настоящее постановление вступает в силу по истечении 6 месяцев со дня его официального опубликования.

Председатель Правительства
Российской Федерации

В. Путин

Москва
6 июля 2008 г.
N 512

**Требования
к материальным носителям биометрических персональных данных
и технологиям хранения таких данных вне информационных
систем персональных данных**

**(утв. постановлением Правительства РФ от 6 июля 2008 г. N 512)
С изменениями и дополнениями от:**

27 декабря 2012 г.

1. Настоящие требования применяются при использовании материальных носителей, на которые осуществляется запись биометрических персональных данных, а также при хранении биометрических персональных данных вне информационных систем персональных данных.
2. В настоящих требованиях под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность (далее - материальный носитель).

3. Настоящие требования не распространяются на отношения, возникающие при использовании:

а) оператором информационной системы персональных данных (далее - оператор) материальных носителей для организации функционирования информационной системы персональных данных, оператором которой он является;

б) бумажных носителей для записи и хранения биометрических персональных данных.

4. Материальный носитель должен обеспечивать:

а) защиту от несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных;

б) возможность доступа к записанным на материальный носитель биометрическим персональным данным, осуществляемого оператором и лицами, уполномоченными в соответствии с законодательством Российской Федерации на работу с биометрическими персональными данными (далее - уполномоченные лица);

в) возможность идентификации информационной системы персональных данных, в которую была осуществлена запись биометрических персональных данных, а также оператора, осуществившего такую запись;

г) невозможность несанкционированного доступа к биометрическим персональным данным, содержащимся на материальном носителе.

5. Оператор утверждает порядок передачи материальных носителей уполномоченным лицам.

6. Материальный носитель должен использоваться в течение срока, установленного оператором, осуществившим запись биометрических персональных данных на материальный носитель, но не более срока эксплуатации, установленного изготовителем материального носителя.

7. Тип материального носителя, который будет использован для обработки биометрических персональных данных, определяет оператор, за исключением случаев, когда нормативными правовыми актами Российской Федерации предписано использование материального носителя определенного типа.

8. Оператор обязан:

а) осуществлять учет количества экземпляров материальных носителей;

б) осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

9. Технологии хранения биометрических персональных данных вне информационных систем персональных данных должны обеспечивать:

а) доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;

Постановлением Правительства РФ от 27 декабря 2012 г. N 1404 в подпункт "б" внесены изменения

См. текст подпункта в предыдущей редакции

б) применение средств электронной подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;

в) проверку наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством Российской Федерации в сфере отношений, связанных с обработкой персональных данных.

Постановлением Правительства РФ от 27 декабря 2012 г. N 1404 в пункт 10 внесены изменения

См. текст пункта в предыдущей редакции

10. В случае если на материальном носителе содержится дополнительная информация, имеющая отношение к записанным биометрическим персональным данным, то такая информация должна быть подписана усиленной квалифицированной электронной подписью и (или) защищена иными информационными технологиями, позволяющими сохранить целостность и неизменность информации, записанной на материальный носитель.

Использование шифровальных (криптографических) средств защиты информации осуществляется в соответствии с законодательством Российской Федерации.

11. При хранении биометрических персональных данных вне информационных систем персональных данных должна обеспечиваться регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

12. Оператор вправе установить не противоречащие требованиям законодательства Российской Федерации дополнительные требования к технологиям хранения биометрических персональных данных вне информационных систем персональных данных в зависимости от методов и способов защиты биометрических персональных данных в информационных системах персональных данных этого оператора.

Постановление Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"

В целях реализации Федерального закона "О персональных данных" Правительство Российской Федерации постановляет:

1. Утвердить прилагаемое Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.
2. Федеральным органам исполнительной власти в месячный срок привести свои акты по вопросам обработки персональных данных, осуществляемой без использования средств автоматизации, в соответствие с настоящим постановлением.
3. Настоящее постановление вступает в силу по истечении одного месяца со дня его официального опубликования.

Председатель Правительства
Российской Федерации

В. Путин

Москва
15 сентября 2008 г.
N 687

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации (утв. постановлением Правительства РФ от 15 сентября 2008 г. N 687)

I. Общие положения

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.
3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов

исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований настоящего Положения.

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

5. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

7. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели 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;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со

своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

9. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

10. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

11. Правила, предусмотренные пунктами 9 и 10 настоящего Положения, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

12. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

13. 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.

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

15. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

**Перечень
мер, направленных на обеспечение выполнения обязанностей,
предусмотренных Федеральным законом "О персональных
данных" и принятыми в соответствии с ним нормативными
правовыми актами, операторами, являющимися государственными
или муниципальными органами**

С изменениями и дополнениями от:

20 июля 2013 г., 6 сентября 2014 г., 15 апреля 2019 г.

1. Операторы, являющиеся государственными или муниципальными органами, принимают следующие меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами:

Подпункт "а" изменен с 25 апреля 2019 г. - Постановление Правительства России от 15 апреля 2019 г. N 454

См. предыдущую редакцию

а) назначают ответственного за организацию обработки персональных данных в государственном или муниципальном органе из числа государственных или муниципальных служащих и (или) работников указанного органа, замещающих должности, не являющиеся должностями государственной гражданской службы Российской Федерации или муниципальной службы, на основании трудового договора (далее - служащие);

Постановлением Правительства РФ от 6 сентября 2014 г. N 911 в подпункт "б" внесены изменения

См. текст подпункта в предыдущей редакции

б) утверждают актом руководителя государственного или муниципального органа следующие документы:

правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований;

правила рассмотрения запросов субъектов персональных данных или их представителей;

правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора;

правила работы с обезличенными данными в случае обезличивания персональных данных;

перечень информационных систем персональных данных;

перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций;

перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных;

перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;

должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе;

типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных, а также типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных;

в) при эксплуатации информационных систем персональных данных в случае, если государственный или муниципальный орган является оператором таких информационных систем, принимают правовые, организационные и технические меры по обеспечению безопасности персональных данных при их обработке, предусмотренные соответствующими нормативными правовыми актами, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных при их обработке, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

г) при обработке персональных данных, осуществляемой без использования средств автоматизации, выполняют требования, установленные постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

д) в целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям организуют проведение периодических проверок условий обработки персональных данных в государственном или муниципальном органе. Проверки осуществляются ответственным за организацию обработки персональных данных в государственном или муниципальном органе либо комиссией, образуемой руководителем государственного или муниципального органа. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, руководителю

государственного или муниципального органа докладывает ответственный за организацию обработки персональных данных в государственном или муниципальном органе либо председатель комиссии;

е) осуществляют ознакомление служащих государственного или муниципального органа, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных и (или) организуют обучение указанных служащих;

ж) уведомляют уполномоченный орган по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных, за исключением случаев, установленных Федеральным законом "О персональных данных";

Постановлением Правительства РФ от 6 сентября 2014 г. N 911 подпункт "з" изложен в новой редакции

См. текст подпункта в предыдущей редакции

з) в случаях, установленных нормативными правовыми актами Российской Федерации, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов персональных данных, осуществляют обезличивание персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ.

2. Документы, определяющие политику в отношении обработки персональных данных, подлежат опубликованию на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения.