

ПРИЛОЖЕНИЕ № 1

УТВЕРЖДЕНЫ

приказом МБДОУ ДС №16

"Петушок" с. Агой

от "09" января 2017 года № 16/7-О

ПРАВИЛА

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 предназначению 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: сотрудники учреждения; воспитанники; родители, законные представители воспитанников.

Настоящие правила определяют необходимый минимальный объем 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) сотрудников 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. Правила обработки персональных данных

Все персональные данные субъектов Учреждение получает на законной основе.

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

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 в соответствии с утверждённым Заведующим списком.

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 специалистов 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, исключающими 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.

Сотрудники 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.

4. 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.

5. 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.

6. 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.

7. 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 сотрудниками 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.

8. 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.

9. 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 .

