

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ДЕТСКИЙ САД № 5 «УЛЫБКА»
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ АБИНСКИЙ РАЙОН



УТВЕРЖДАЮ

Заведующий

МБДОУ детский сад № 5

Н.Г. Ширяева Н.Г. Ширяева

«11» *сентября* 2021 г.

приказ № *37* от *11.01.2021* г.

**Правила
обработки персональных данных**

г. Абинск

1. Общие положения

1.1. Настоящие Правила обработки персональных данных (далее – Правила) разработаны для муниципального бюджетного дошкольного образовательного учреждения детского сада № 5 «Улыбка» муниципального образования Абинский район (далее – ДОО).

1.2. Настоящие Правила устанавливают единый порядок обработки персональных данных и обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации и без использования средств автоматизации в ДОО.

1.3. Настоящие Правила разработаны в соответствии с требованиями следующих законодательных и нормативных правовых актов Российской Федерации:

- Трудовой кодекс Российской Федерации (статья 65, статьи 85 – 90);
- Федеральный закон от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- постановление Правительства Российской Федерации от 15.09.2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановление Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.4. Настоящие Правила устанавливают и определяют:

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

1.5. В настоящих Правилах используются следующие понятия:

- оператор – ДОО, организующая и осуществляющая обработку персональных данных, а также определяющая цели и содержание обработки персональных данных;
- персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата

и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

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

- информационная система персональных данных (далее – информационная система) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

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

- 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;

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

- обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

- обработка персональных данных без использования средств автоматизации (далее – неавтоматизированный способ) – действия с персональными данными, такие как сбор, систематизация, накопление, хранение, использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека;

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

- распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой

информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта персональных данных;

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

1.6. ДОО является оператором персональных данных, осуществляющим обработку персональных данных работников ДОО и лиц, не являющихся работниками ДОО: воспитанников и их родителей (законных представителей).

1.7. Доступ к Правилам неограничен, так как Правила являются документом, определяющим политику ДОО в отношении обработки персональных данных.

1.8. Настоящие Правила являются обязательными для исполнения всеми работниками ДОО, имеющими доступ к персональным данным.

1.9. Работники, определенные приказом руководителя ДОО, как пользователи, участвующие в обработке персональных данных, должны ознакомиться с настоящими Правилами.

1.10. Обязанность доводить до сведения работников ДОО положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных лежит на лице, ответственном за организацию обработки персональных данных (пункт 2, часть 4, статья 22.1 Федерального закона №152-ФЗ).

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

2. Процедуры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством Российской Федерации в сфере персональных данных

2.1. ДОО должно соблюдать принципы и условия обработки персональных данных, а также права субъектов персональных данных, определенные в Федеральном законе №152-ФЗ.

2.2. ДОО должно принимать меры, направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом №152-ФЗ в частности:

- назначить ответственного за организацию обработки персональных данных в ДОО;

- разработать и утвердить документы, определяющие политику ДОО в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона №152-ФЗ;
- осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону №152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам ДОО;
- оценивать вред, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации и настоящих Правил;
- ознакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных и настоящими Правилами;
- запрещать обработку персональных данных лицами, не допущенными к их обработке.

2.3. Обработка персональных данных должна осуществляться после получения согласия субъекта персональных данных (за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона №152-ФЗ), при условии выполнения требований к защите персональных данных.

2.4. Безопасность персональных данных при их обработке в информационной системе обеспечивает ДОО.

2.5. При обработке персональных данных необходимо соблюдать следующие требования:

- к работе с персональными данными допускаются только лица, назначенные соответствующим приказом руководителя ДОО;
- в целях обеспечения сохранности документов, содержащих персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться работниками ДОО, осуществляющими данную работу в соответствии со своими должностными обязанностями, зафиксированными в их должностных инструкциях;
- на период обработки защищаемой информации в помещении могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации.

2.6. Особенности обработки персональных данных с использованием средств автоматизации:

- обработка персональных данных с использованием средств автоматизации осуществляется в информационных системах персональных данных, состав которых должен быть определен в Перечне информационных систем персональных данных;
- машинные носители персональных данных должны подлежать обязательной регистрации и учету в соответствии с приказом руководителя ДОО, регламентирующим порядок учета и хранения носителей персональных данных;
- обработка персональных данных должна осуществляться при условии выполнения требований к защите персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных. Состав и содержание таких мер утвержден приказом ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2.7. Особенности обработки персональных данных без использования средств автоматизации изложены в постановлении Правительства Российской Федерации от 15.09.2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

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

- персональные данные при их обработке должны обособляться от иной информации, в частности, путем фиксации их на отдельных носителях;
- при фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы;
- для обработки различных категорий персональных данных для каждой категории персональных данных должен использоваться отдельный материальный носитель;
- лица, осуществляющие обработку персональных данных, 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 ДОО;

- требования к типовым формам документов, характер информации в которых предполагает или допускает включение в них персональных данных, изложены в пункте 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного Постановлением Правительства Российской Федерации от 15.09.2008 года № 687;
- уточнение персональных данных 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.

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

- обработка персональных данных 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;
- необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
- при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ.

3. Цель обработки персональных данных

3.1. Цель обработки персональных данных определяется целями создания и видами деятельности ДОО, а именно соблюдение действующего законодательства.

3.2. Субъектами, персональные данные которых обрабатываются для указанных целей, являются работники ДОО, а также лица, не являющиеся работниками ДОО: воспитанники и их родители (законные представители).

4. Содержание обрабатываемых персональных данных для каждой цели обработки персональных данных

4.1. Содержание обрабатываемых персональных данных должно определяться целью обработки персональных данных и утверждаться локальным актом ДОО – Перечнем персональных данных, обрабатываемых в ДОО в связи с реализацией трудовых и служебных отношений, а также в связи с оказанием услуг.

4.2. Содержание обрабатываемых персональных данных определяется для каждой цели обработки персональных данных.

5. Категории субъектов персональных данных

5.1. Категории субъектов, персональные данные которых обрабатываются:

- работники ДОО;
- лица, не являющиеся работниками ДОО: воспитанники и их родители (законные представители).

6. Порядок обработки персональных данных

6.1. Обработка персональных данных в информационных системах ДОО должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям ДОО;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

6.2. Обработка персональных данных в информационных системах ДОО может осуществляться ДОО с письменного согласия субъектов персональных данных, за исключением следующих случаев, когда такого согласия не требуется, если:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных

и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно.

6.3. Обработка оператором специальных категорий персональных данных в информационных системах ДОО допускается если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;
- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья субъекта персональных данных и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта персональных данных невозможно.

6.4. В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

6.5. Оператор, получающий доступ к персональным данным, должен обеспечивать конфиденциальность таких данных, за исключением случаев:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

6.6. Обработка персональных данных в информационных системах ДОО осуществляется только с согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных федеральными законами, которыми предусматриваются случаи обязательного предоставления субъектом персональных данных своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

6.7. Письменное согласие субъекта персональных данных на обработку своих персональных данных в информационных системах ДОО должно включать в себя:

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

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

6.8. Обязанность предоставить доказательство получения согласия субъекта персональных данных на обработку его персональных данных, а в случае обработки общедоступных персональных данных в информационных системах ДОО обязанность доказывания того, что обрабатываемые персональные данные являются общедоступными, возлагается на оператора.

6.9. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных в информационных системах ДОО дает в письменной форме законный представитель субъекта персональных данных.

6.10. В случае смерти субъекта персональных данных согласие на обработку его персональных данных в информационных системах ДОО дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

6.11. Субъект персональных данных имеет право на получение сведений об обработке своих персональных данных в информационных системах ДОО, а оператор обязан их предоставить в соответствии со статьями 14 и 20 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

7. Сроки обработки и хранения обрабатываемых персональных данных

7.1. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных.

7.2. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

7.3. Основания для прекращения обработки персональных данных и сроки их уничтожения определены в частях 3, 4, 5 статьи 21 Федерального закона №152-ФЗ.

7.4. Основанием (условием) прекращения обработки персональных данных также является ликвидация ДОО.

7.5. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3, 4, 5 статьи 21 Федерального закона №152-ФЗ, ДОО осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению ДОО) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8. Меры по обеспечению безопасности персональных данных при их обработке

8.1. Безопасность персональных данных, обрабатываемых в информационных системах ДОО, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

8.2. Для обеспечения безопасности персональных данных при их обработке в информационных системах ДОО осуществляется защита:

- информации, обрабатываемой с использованием технических средств;
- информации, содержащейся на бумажной, магнитной, магнитно-оптической и иной основе (носителях).

8.3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах ДОО являются неотъемлемой частью работ по созданию информационных систем.

8.4. Информационные системы ДОО классифицируются оператором. Проведение классификации информационных систем определено Порядком проведения классификации информационных систем персональных данных, утвержденным совместным приказом Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерством информационных технологий и связи Российской Федерации от 13.02.2008 года № 55/86/20.

8.5. Обмен персональными данными при их обработке в информационных системах ДОО осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических и программных средств.

8.6. Размещение информационных систем ДОО, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны

обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.7. Безопасность персональных данных при их обработке в информационных системах ДОО обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее – уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

8.8. При обработке персональных данных в информационных системах ДОО безопасность обеспечивается:

- проведением мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременным обнаружением фактов несанкционированного доступа к персональным данным;
- недопущением воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможностью незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянным контролем за обеспечением уровня защищенности персональных данных.

8.9. Защита персональных данных, обрабатываемая в информационных системах ДОО, обеспечивается за счет средств ДОО в порядке, установленном федеральными законами.

8.10. Доступ работников ДОО к персональным данным, обрабатываемым в информационных системах ДОО, для выполнения своих должностных обязанностей производится к соответствующим персональным данным на основании списка, утвержденного оператором.

9. Порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований

9.1. При уничтожении материальных носителей, содержащих персональные данные, должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

9.2. Уничтожение части персональных данных, если это допускается материальным носителем, может производиться способом, исключаящим

дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

9.3. Для уничтожения персональных данных ДОО создает комиссию. В состав комиссии включается ответственное лицо за организацию обработки персональных данных. Уничтожение персональных данных производится в присутствии всех членов комиссии.

9.4. После уничтожения материальных носителей членами комиссии подписывается Акт об уничтожении персональных данных.

10. Ответственность за нарушение требований законодательства в сфере защиты персональных данных

10.1. Ответственность за обеспечение безопасности персональных данных и надлежащий режим работы информационных систем ДОО возлагается на руководителя ДОО.

10.2. В своей работе работники ДОО, допущенные к обработке персональных данных в информационных системах ДОО, должны руководствоваться требованиями федеральных законов, нормативно-правовых документов Правительства Российской Федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации, а также настоящими Правилами.

10.3. В должностные инструкции работников ДОО, уполномоченных на обработку персональных данных в информационных системах ДОО, должны быть внесены обязанности о необходимости выполнения требований по обеспечению безопасности обрабатываемых ими персональных данных.

10.4. Ответственное лицо за обеспечение безопасности персональных данных в ДОО руководствуется в своей деятельности инструкцией ответственного лица за обеспечение безопасности персональных данных, обрабатываемых ДОО.

10.5. При обнаружении нарушений порядка предоставления персональных данных, ДОО незамедлительно приостанавливает предоставление персональных данных до выявления причин нарушений и устранения этих причин.

10.6. За нарушение норм настоящих Правил, а также федеральных законов, регламентирующих порядок обработки и обеспечения безопасности персональных данных, работники ДОО, допущенные к работе с персональными данными, несут гражданско-правовую, административную, уголовную и дисциплинарную ответственность в соответствии с действующим законодательством.