

Положение
о порядке организации и проведению работ
по защите персональных данных
Муниципальное автономное дошкольное образовательное учреждение
«Золушка» муниципального образования город Ноябрьск

Положение о порядке организации и проведению работ по защите персональных данных

Муниципальное автономное дошкольное образовательное учреждение «Золушка» муниципального образования город Ноябрьск

Общие положения

- 1.1. Настоящее Положение разработано в соответствии с Федеральным законом 152-ФЗ «О персональных данных» (далее Федеральный закон), постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемо использования средств автоматизации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационной системе персона вных данных.
- 1.2. Настоящее Положение регулирует отношения, связанные с обработкой персональных данных, осуществляемой с использованием средств автоматизации и и без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаем с персональными данными с использованием средств автоматизации, в информаци нной системе Муниципального автономного дошкольного образовательного учреж цения «Золушка» муниципального образования город Ноябрьск, являющейся информаци нной системой персональных данных (ИСПДн).
 - 1.3. В Положении используются следующие термины и их определения:
- 1) персональные данные любая информация, относящаяся к прямо или коспенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 2) информационная система персональных данных (ИСПДн) совоку ность содержащихся в базах данных персональных данных и обеспечивающих их образотку информационных технологий и технических средств;
- 3) *оператор* (здесь) самостоятельно или совместно с другими лими организующие и (или) осуществляющие обработку персональных данных, а акже определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данным п
- 4) обработка персональных данных любое действие (операция) или совокут ность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, з пись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извление, использование, передачу (распространение, предоставление, доступ), обезличие, блокирование, удаление, уничтожение персональных данных;
- 4) автоматизированная обработка персональных данных обработка персональных данных с помощью средств вычислительной техники;
- 5) распространение персональных данных действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
- 6) *предоставление персональных данных* действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
- 7) *блокирование персональных данных* временное прекращение обработки персональных данных (за исключением случаев, если обработка необходим уточнения персональных данных);
- 8) уничтожение персональных данных действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной стеме персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- 9) обезличивание персональных данных действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных
- 10) трансграничная передача персональных данных передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

1. Основные положения защиты персональных данных

- 1.1. Цели и содержание обработки персональных данных определяются в соответствии с требованиями законодательства РФ.
- 1.2. Обработка персональных данных в организации осуществляется в соответитвии с утвержденной организационно-распорядительной документацией, определяющей правила и процедуры работы с персональными данными.
- 1.3. Защищаемая информация в организации определяется в соответствии с Перечнем сведений, подлежащих защите.
- 1.4. Безопасность персональных данных в организации при их обработке обеспечивает подразделение, осуществляющее обработку персональных данных.
- 1.5. Безопасность персональных данных при их обработке в информаци нной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 стать 19 Федерального закона «О персональных данных».
- 1.6. Система защиты персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасиссти персональных данных и информационных технологий, используемых в информационных системах.
- 1.7. Выбор средств защиты информации для системы защиты персональных данных осуществляется уполномоченным лицом оператора по защите ПДн и согласуе ся с отделом информационной безопасности.
- 1.8. ИСПДн является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные да ные, касающиеся расовой, национальной принадлежности, политических взг. ядов, религиозных или философских убеждений, состояния здоровья, интимной субъектов персональных данных.
- 1.9. ИСПДн является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характер зуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления лич субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.
- 1.10. ИСПДн является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального зако на персональных данных».
- 1.11. ИСПДн является информационной системой, обрабатывающей категории персональных данных, если в ней не обрабатываются специальные категории персональных данных, биометрические персональные данные или общедост пые персональные данные.
- 1.12. ИСПДн является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные трько указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

2. Основные положения обработки персональных данных

- 3.1. Обработка персональных данных в ИСПДн осуществляется в соответствии с требованиями Федерального закона «О персональных данных», нормативно и методических документов уполномоченных федеральных органов исполнительной и исти по обеспечению безопасности персональных данных, а так же нормативно-правовыми актами и организационно-распорядительными документами организации.
- 3.2. Оператором осуществляется определение уровня защищенности П. П в соответствии с Постановлением Правительства российской Федерации от 01.1 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработ ке в информационных системах персональных данных» в зависимости от типа угроз, кате ории обрабатываемых данных и их объема. Результаты определения уровня защищенности оформляются Актом и утверждаются руководителем организации.
- 3.3. Приказом руководителя назначается сотрудник, ответственный за защиту персональных данных (администратор безопасности ПДн), определяется перечень помещений, в которых разрешена обработка ПДн, и перечень должностных лиц, уполномоченных на обработку персональных данных и (или) имеющих доступ к персональным данным.
- 3.4. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением и подписывают обязательство о неразглашение информации, содержащей персональные данные.

3. Порядок обработки персональных данных

- 4.1. Персональные данные граждан (субъектов ПДн), не являю и хся сотрудниками оператора, обрабатываются строго в связи с осуществлением и выполнением возложенных на него функций, полномочий и обязанностей.
- 4.2. Требования к обработке оператором иных категорий персональных динных идентичны п.4 настоящего Положения.
- 4.3. Субъект ПДн имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:
 - 1) подтверждение факта обработки персональных данных оператором;
 - 2) правовые основания и цели обработки персональных данных;
 - 3) цели и применяемые оператором способы обработки ПДн;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или корым могут быть раскрыты персональные данные на основании договора с оператором и п на основании федерального закона;
- 5) обрабатываемые персональные данные, относящиеся к соответствук пему субъекту персональных данных, источник их получения, если иной порядок предстантения таких данных не предусмотрен федеральным законом;
 - 6) сроки обработки персональных данных, в том числе сроки их хранения;
- 7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;
- 8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- 9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена будет поручена такому лицу;
- 10) иные сведения, предусмотренные настоящим Федеральным законом другими федеральными законами.
- 4.4. Право субъекта ПДн на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:
- 1) обработка персональных данных, полученных в результате опера и норозыскной, контрразведывательной и разведывательной деятельности, осуществля в целях обороны страны, безопасности государства и охраны правопорядка;

- 2) обработка персональных данных осуществляется органами, осуществин и ими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с так ими персональными данными;
- 3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- 4) доступ субъекта персональных данных к его персональным данным нар права и законные интересы третьих лиц;
- 5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в пелях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.
- 4.5. Оператор обязан немедленно прекратить по требованию субъекта ПДн обработку его персональных данных.

4. Порядок обработки персональных данных с использованием средств автоматизации

- 4.1. Обработка персональных данных с использованием средств автомати а дии осуществляется в соответствии с требованиями постановления Правительства Росси ской Федерации от 1 ноября 2012 г. № 1119, нормативных и методических докумин тов уполномоченных федеральных органов исполнительной власти по обеспечению безопасности персональных данных, а так же нормативно-правовыми актами и организационно-распорядительными документами организации.
- 4.2. Требования к защите персональных данных в ИСПДн определяются исходя из определенного уровня защищенности ПДн и состава актуальных угроз безопас ости персональным данным.
- 4.3. Под актуальными угрозами безопасности персональных данных понимаются совокупность условий и факторов, создающих актуальную опасиссть несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которой могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.
- 4.4. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных».
- 4.5. Для обеспечения требуемого уровня защищенности персональных данных их обработке в ИСПДн необходимо выполнение следующих требований:
- а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируем ого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа оти помещения;
 - б) обеспечение сохранности носителей персональных данных;
- в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- г) использование средств защиты информации, прошедших процедуру опракти соответствия требованиям законодательства Российской Федерации в области

обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- д) назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе;
- е) поддержание в актуальном состоянии электронного журнала сообщений, определенного постановлением Правительства РФ от 1 ноября 2012 г. № 1119.
- 4.6. Не допускается обработка персональных данных в ИСПДн с использов нием средств автоматизации при отсутствии:
- утвержденной организационно-распорядительной документации о порядке р боты и защиты ПДн в организации, включающих акт классификации ИСПДн, инструкции пользователя, администратора безопасности, по организации антивирусной защиты, использования средств защиты информации и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;
- охраны и организации режима допуска к ресурсам ИСПДн и в помещения, предназначенные для обработки персональных данных.
- 4.7. Запрещается принятие на основании исключительно автоматизиров нной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и зак и ные интересы.
- 4.8. Решение, порождающее юридические последствия в отношении субъекта ПДн 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 ПДн или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта ПДн.
- 4.9. Оператор обязан разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность за пить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов.
- 4.10. Оператор обязан рассмотреть возражение, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

5. Порядок обработки персональных данных без использования средств автоматизации

- 5.1. Обработка персональных данных без использования средств автомати зации (неавтоматизированная) обработка персональных данных, содержащих я в информационной системе персональных данных либо извлеченных из такой системь ссли такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.
- 5.2. Обработка персональных данных без использования средств автомати зации (далее неавтоматизированная обработка персональных данных) может осуществля в звиде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.
- 5.3. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.
- 5.4. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.
- 5.5. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее типовые формы), 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 неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилик, 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 персонать ных данных может поставить отметку о своем согласии на неавтоматизированную обрать тку персональных данных, 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 несовместимы.
- 5.6. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних электронных носителях информации.
- 5.7. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внаш них носителях информации необходимо принимать организационные (охрана помещев ий) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данный лиц, не допущенных к их обработке.
- 5.8. Электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных. К катдому электронному носителю оформляется опись файлов, содержащихся на нем, с указанием цели обработки и категории персональных данных.
- 5.9. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от эругих зафиксированных на том же носителе персональных данных, должны быть принять по обеспечению раздельной 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 динных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.
- 5.10. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в напекно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

6. Меры, направленные на обеспечение безопасности ПДн

- 6.1. Оператор обязан принимать меры, необходимые и достаточные для обеспечения безопасности персональных данных.
 - 6.2. Обеспечение безопасности персональных данных достигается:
- 1) определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- 2) применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством РФ урс вни защищенности персональных данных;
- 3) применением прошедших в установленном порядке процедуру от кнки соответствия средств защиты информации;
- 4) оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
 - 5) учетом машинных носителей персональных данных;
- 6) обнаружением фактов несанкционированного доступа к персональным дань м и принятием мер;
- 7) восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- 8) установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;
- 9) контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
 - 6.3. К мерам обеспечения безопасности персональных данных относятся:
- 1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;
- 2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений:
- 3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;
- 4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

- 5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанных предусмотренных настоящим Федеральным законом;
- 6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федетации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных работников.
- 6.4. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персонать ных данных, к сведениям о реализуемых требованиях к защите персональных данных.
- 6.5. Оператор обязан представить документы и локальные акты и (или) иным образом подтвердить принятие мер по запросу уполномоченного органа по защите грав субъектов персональных данных.
- 6.6. Для выполнения работ и оказания услуг по обеспечению безопасти персональных данных могут привлекаться на договорной основе специализиров ные организации лицензиаты ФСТЭК России по технической защите конфиденция вной информации.

7. Порядок контроля и ответственность должностных лиц

- 9.1. Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имерщих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в роки, определяемые оператором (уполномоченным лицом).
- 9.2. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных в государственных информации ных системах персональных данных осуществляются федеральным органом исполните вной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий и без права ознакомления с персональными данными, обрабатываемыми в информационных системах персональных данных.
- 9.3. Субъект ПДн имеет право на защиту своих прав и законных интересов в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном по идке.
- 9.4. Сотрудники организации, допущенные установленным порядком к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, граждан коправовую или уголовную ответственность в соответствии с законодательством Российской Федерации.