УТВЕРЖДАЮ
Директор
МАУ ДО Нижнетавдинского
муниципального района «ЦДО»:
_____ С.С. Федотова
«30» 01 2025 г.

Положение о защите, хранении и обработке персональных данных клиентов и контрагентов МАУ ДО Нижнетавдинского муниципального района «ЦДО»

1. Общие положения

1.1. Настоящее положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных), Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства РФ от 1 ноября 2012 г. N 1119, и иными нормативными актами в области защиты персональных данных, действующими на территории Российской Федерации.

1.2. Настоящее положение устанавливает порядок обработки персональных данных клиентов и контрагентов **МАУ ДО Нижнетавдинского муниципального района «ЦДО** (далее - организация), основные цели, принципы обработки и требования к безопасности персональных данных.

1.3. Настоящее положение разработано в целях регулирования порядка сбора, систематизации, хранения, передачи и уничтожения персональных данных клиентов и контрагентов организации.

2. Понятие и состав персональных данных

2.1. В целях настоящего положения под персональными данными понимается любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.2. К персональным данным клиента относятся:
- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.);
- паспортные данные;
- адрес регистрации;
- адрес места жительства;
- номер телефона;

2.3. К персональным данным контрагента относятся:
- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.);
- паспортные данные;
- адрес регистрации;
- адрес места жительства;
- номер телефона;
- сведения о номере и серии страхового свидетельства государственного пенсионного страхования;
- сведения об идентификационном номере налогоплательщика;

2.4. Указанные сведения и документы являются конфиденциальными. Организация как оператор персональных данных не вправе распространять персональные данные без согласия клиента или контрагента, если иное не предусмотрено федеральным законом.

3. Обработка персональных данных и гарантии их защиты

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

3.2. В целях обеспечения прав и свобод человека и гражданина организация при обработке персональных данных клиента или контрагента соблюдает следующие общие требования:

- обработка персональных данных клиента или контрагента осуществляется исключительно в целях обеспечения соблюдения законов.

- при определении объема и содержания обрабатываемых персональных данных клиента или контрагента организация руководствуется Конституцией Российской Федерации и иными федеральными законами;

- все персональные данные клиента или контрагента следует получать у него самого. Если персональные данные клиента или контрагента возможно получить только у третьей стороны, то клиент или контрагент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Организация сообщает клиенту или контрагенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа клиента или контрагента дать письменное согласие на их получение;

- организация не вправе получать и обрабатывать персональные данные клиента или контрагента о его политических, религиозных и иных убеждениях и частной жизни;

- организация не вправе получать и обрабатывать персональные данные клиента или контрагента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

3.3. Защита персональных данных клиента или контрагента от неправомерного их использования или утраты обеспечивается организацией за счет ее средств в порядке, установленном федеральными законами и настоящим положением.

3.4. Клиенты и контрагенты организации должны быть ознакомлены под роспись с документами организации, устанавливающими порядок обработки персональных данных клиентов и контрагентов, а также об их правах и обязанностях в этой области.

3.5. Организация при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает 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.

3.6. Организация осуществляет **внутренний контроль** соответствия обработки персональных данных Закону о персональных данных, требованиям к защите персональных данных, политике организации в отношении обработки персональных данных, настоящему положению.

3.7. Организация знакомит работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучает указанных работников.

3.8. Организация обеспечивает безопасность персональных данных клиента или контрагента следующими способами:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- 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 Российской Федерации уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- 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;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

3.9. Организация обрабатывает в информационных системах с использованием средств автоматизации следующие категории персональных данных клиента, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных:

3.10. Организация обрабатывает в информационных системах с использованием средств автоматизации следующие категории персональных данных контрагента, обеспечивает их защиту с учетом определенного типа угроз безопасности и уровня защищенности персональных данных.

3.11. При 4-м уровне защищенности персональных данных организация:

- обеспечивает режим безопасности помещений, в которых размещена информационная система, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечивает сохранность носителей персональных данных;

- утверждает перечень работников, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- использует средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

3.12. При 3-м уровне защищенности персональных данных организация дополнительно к мерам, перечисленным в пункте 3.11 настоящего положения, назначает должностное лицо (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.

3.13. При 2-м уровне защищенности персональных данных организация дополнительно к мерам, перечисленным в пунктах 3.11, 3.12 настоящего положения, ограничивает доступ к содержанию электронного журнала сообщений, за исключением для должностных лиц (работников), которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

3.14. При 1-м уровне защищенности персональных данных организация дополнительно к мерам, перечисленным в пунктах 3.11-3.13 настоящего положения:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работника по доступу к персональным данным, содержащимся в информационной системе;

- создает структурное подразделение, ответственное за обеспечение безопасности персональных данных в информационной системе, либо возлагает на одно из структурных подразделений функции по обеспечению такой безопасности.

3.15. Организация при обработке персональных данных клиента или контрагента на бумажных носителях в целях обеспечения их защиты:

- назначает должностное лицо (работника), ответственного за обработку персональных данных;

- ограничивает допуск в помещения, в которых хранятся документы, содержащие персональные данные клиентов и контрагентов.

3.19. Работники, допущенные к персональным данным клиентов и контрагентов, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки персональных данных клиентов и контрагентов не допускаются.

3.20. Персональные данные клиентов и контрагентов на бумажных носителях хранятся в сейфе. Право доступа к персональным данным имеют:

- руководитель организации;

- делопроизводитель;

- старший методист;

- главный бухгалтер;

- педагоги дополнительного образования.

3.21. Персональные данные клиентов и контрагентов в электронном виде хранятся в локальной компьютерной сети организации, в электронных папках и файлах в персональных компьютерах и работников, допущенных к обработке персональных данных клиентов и контрагентов.

4. Передача персональных данных

4.1. При передаче персональных данных клиента или контрагента организация соблюдает следующие требования:

- не сообщать персональные данные клиента или контрагента третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью клиента или контрагента, а также в других случаях, установленных федеральными законами;
- не сообщать персональные данные клиента или контрагента в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные клиента или контрагента, 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 клиента или контрагента, обязаны соблюдать режим секретности (конфиденциальности);
- разрешать доступ к персональным данным клиентов и контрагентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные клиентов и контрагентов, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья клиентов и контрагентов.

4.2. Все сведения о передаче персональных данных клиента или контрагента учитываются для контроля правомерности использования данной информации лицами, ее получившими.

4.3. Передача персональных данных по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством Российской Федерации, допускается исключительно с согласия клиента или контрагента на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

4.4. Передача информации, содержащей сведения о персональных данных клиента или контрагента, по телефону, в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

4.5. Согласие на обработку персональных данных, разрешенных клиентом или контрагентом для распространения, оформляется отдельно от иных согласий клиента или контрагента на обработку его персональных данных. Организация обеспечивает клиенту или контрагенту возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных им для распространения.

4.6. В согласии на обработку персональных данных, разрешенных клиентом или контрагентом для распространения, он вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных организацией неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

4.7. Передача (распространение, предоставление, доступ) персональных данных, разрешенных клиентом или контрагентом для распространения, должна быть прекращена в любое время по его требованию. Указанные в данном требовании персональные данные могут обрабатываться только организацией.

5. Порядок уничтожения персональных данных

5.1. В случае выявления неправомерной обработки персональных данных при обращении клиента или контрагента организация осуществляет блокирование неправомерно обрабатываемых персональных данных, относящихся к этому клиенту или контрагенту, с момента такого обращения на период проверки.

5.2. В случае выявления неточных персональных данных при обращении клиента или контрагента организация осуществляет блокирование персональных данных, относящихся к этому клиенту или контрагенту, с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы клиента или контрагента, или третьих лиц.

5.3. В случае подтверждения факта неточности персональных данных организация на основании

сведений, представленных клиентом или контрагентом, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

5.4. В случае выявления неправомерной обработки персональных данных, осуществляемой организацией, организация в срок, не превышающий трех рабочих дней с даты этого выявления, прекращает неправомерную обработку персональных данных.

5.5. В случае если обеспечить правомерность обработки персональных данных невозможно, организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

5.6. Об устранении допущенных нарушений или об уничтожении персональных данных организация уведомляет клиента или контрагента.

5.7. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав клиента или контрагента, организация с момента выявления такого инцидента организацией, уполномоченным органом по защите прав субъектов персональных данных или иным заинтересованным лицом уведомляет уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав клиента или контрагента, и предполагаемом вреде, нанесенном правам клиента или контрагента, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставляет сведения о лице, уполномоченном организацией на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставляет сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

5.8. В случае достижения цели обработки персональных данных организация прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

5.9. В случае отзыва клиентом или контрагентом согласия на обработку его персональных данных организация прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

5.10. В случае обращения клиента или контрагента в организацию с требованием о прекращении обработки персональных данных организация в срок, не превышающий десяти рабочих дней с даты получения им соответствующего требования, прекращает их обработку, за исключением случаев, предусмотренных Законом о персональных данных.

Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления организацией в адрес клиента или контрагента мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

5.11. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 5.4-5.10 настоящего положения, организация осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

5.12. Организация уведомляет Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций о факте неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав клиентов и контрагентов, в порядке, утвержденном приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 ноября 2022 г. N 187.

5.13. Организация передает в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, информацию о компьютерных инцидентах, повлекших неправомерную или случайную передачу (предоставление, распространение, доступ) персональных данных, в порядке, установленном совместно федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и уполномоченным органом по защите прав субъектов персональных данных.

5.14. После истечения срока нормативного хранения документов, содержащих персональные данные клиента или контрагента, или при наступлении иных законных оснований документы подлежат

уничтожению.

5.15. Организация для этих целей создает экспертную комиссию и проводит экспертизу ценности документов.

5.16. По результатам экспертизы документы, содержащие персональные данные клиента или контрагента и подлежащие уничтожению:

- на бумажном носителе - уничтожаются путем измельчения в шредере.

- в электронном виде - стираются с информационных носителей либо физически уничтожаются сами носители, на которых хранится информация.

5.17. В случае если обработка персональных данных осуществлялась организацией без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных клиентов и контрагентов, является акт об уничтожении персональных данных.

5.18. В случае если обработка персональных данных осуществлялась организацией с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных клиентов и контрагентов, являются акт об уничтожении персональных данных и выгрузка из журнала регистрации событий в информационной системе персональных данных.

6. Права клиентов и контрагентов в целях обеспечения защиты персональных данных

6.1. В целях обеспечения защиты персональных данных, хранящихся в организации, клиенты и контрагенты имеют право на:

- полную информацию об их персональных данных и обработке этих данных, в том числе содержащую:

подтверждение факта обработки персональных данных организацией;

правовые основания и цели обработки персональных данных;

цели и применяемые организацией способы обработки персональных данных;

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

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

информацию о способах исполнения организацией обязанностей, установленных статьей 18.1 Закона о персональных данных;

- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные клиента или контрагента, за исключением случаев, предусмотренных федеральным законом;

- определение своих представителей для защиты своих персональных данных;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Закона о персональных данных. При отказе организации исключить или исправить персональные данные клиента или контрагента он имеет право заявить в письменной форме организации о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера клиент или контрагент имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требование об извещении организацией всех лиц, которым ранее были сообщены неверные или неполные персональные данные клиента или контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия организации при обработке и защите персональных данных.

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

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных клиентов и контрагентов организации, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном федеральными законами РФ, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.2. Моральный вред, причиненный клиенту или контрагенту вследствие нарушения его прав,

нарушения правил обработки персональных данных, установленных федеральным законодательством, а также требований к защите персональных данных, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных клиентом или контрагентом убытков.

8. Заключительные положения

8.1. Настоящее положение вступает в силу с момента его утверждения.

8.2. Организация обеспечивает неограниченный доступ клиентов и контрагентов к настоящему документу.

8.3. Настоящее положение является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным клиента или контрагента, и доводится до их сведения персонально под роспись.

С положением ознакомлены:

N п/п	Ф. И. О.	Дата	Подпись
1	2	3	4