

**Порядок обработки персональных данных
в ГБУ «Комплексный центр социального обслуживания населения
«Мыза» Приокского района города Нижнего Новгорода»**

1. Общие положения

1.1. Порядок обработки персональных данных в ГБУ «Комплексный центр социального обслуживания населения «Мыза» Приокского района города Нижнего Новгорода» (далее – Порядок) разработан в соответствии с Конституцией Российской Федерации, Перечнем сведений конфиденциального характера, утвержденным Указом Президента Российской Федерации от 06.03.1997 N 188 (ред. от 23.09.2005), Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Постановление Правительства Российской Федерации от 15.09.2008 N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Постановлением Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Порядок обязателен для исполнения всеми сотрудниками ГБУ «Комплексный центр социального обслуживания населения «Мыза» Приокского района города Нижнего Новгорода» (далее - Учреждение), чьи должностные обязанности предусматривают выполнение функций по обработке персональных данных, определенных Положением по обработке персональных данных получателей социальных услуг, утверждаемым приказом директором Учреждения.

1.3. Ответственность за организацию выполнения требований законодательства Российской Федерации при работе с персональными данными возлагается на директора Учреждения.

1.4. Контроль выполнения организационных и технических мероприятий при обработке персональных данных, в том числе связанных с обеспечением безопасности персональных данных, осуществляет ответственный за организацию обработки персональных данных, ответственные за обработку персональных данных в подразделениях Учреждения, ответственный за информационную безопасность (в том числе за защиту персональных данных, за исключением сведений, составляющих государственную тайну) в Учреждении (далее - Ответственный за ИБ) и уполномоченные сотрудники подразделения, обеспечивающего информационную безопасность (в том числе защиту персональных данных, за исключением сведений, составляющих государственную тайну) в Учреждении (далее - Подразделение ЗИ).

1.5. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания, если иное не определено законом.

2. Цели задачи обработки персональных данных

2.1. Обработка персональных данных в Учреждении осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", постановлением Правительства Российской Федерации от 06.07.2008 № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", постановлением Правительства Российской Федерации от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", Федеральными законами от 28.12.2013 № 442-ФЗ "Об основах социального обслуживания граждан в Российской Федерации", Законом Нижегородской области от 05.11.2014 № 146-З "О социальном обслуживании граждан в Нижегородской области" и другими нормативными актами.

2.2. При обработке персональных данных в Учреждении достигается решение следующих задач:

- защита конституционных прав граждан Нижегородской области в сфере социального обслуживания;
- участие в осуществлении нормативного правового регулирования в сфере социального обслуживания;
- формирование и развитие оптимальной сети государственных учреждений всех типов, подведомственных Министерству, повышение эффективности их работы, координация и методическое обеспечение их деятельности, развитие новых форм и видов социального обслуживания граждан;
- профилактика социального сиротства, безнадзорности и правонарушений несовершеннолетних, обеспечение условий для социальной реабилитации детей, находящихся в трудной жизненной ситуации и социально опасном положении.

3. Категории субъектов персональных данных, источники получения персональных данных, сроки обработки и хранения персональных данных

3.1. В рамках целей и задач Учреждением обрабатываются персональные данные следующих категорий субъектов персональных данных:

- получатели социальных услуг;
- обратившиеся в Учреждение с обращением, жалобой или заявлением;

3.2. Сроки обработки и хранения персональных данных определены в Номенклатуре дел Учреждения.

4. Принципы обработки персональных данных

4.1. Сбор, обработка персональных данных в Учреждении осуществляется в соответствии с требованиями действующего законодательства Российской Федерации.

4.2. Обработка персональных данных в Учреждении осуществляется на основе следующих 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 оператора;
- 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;

4.3. Учреждение в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в статье 5 Федерального закона 152-ФЗ "О персональных данных";

4.4. Учреждение не осуществляет обработку биометрических персональных данных (сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность);

4.5. Учреждение не выполняет обработку специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни;

4.6. Учреждение не производит трансграничную (на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу) передачу персональных данных;

4.7. Учреждение производит передачу персональных данных третьим лицам на основании соответствующего соглашения и только с согласия субъектов персональных данных;

4.8. Хранение персональных данных в Учреждении осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки. Персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

5. Условия обработки персональных данных

5.1. Обработка персональных данных в Учреждении осуществляется в соответствии с действующим законодательством Российской Федерации.

5.2. В случае если обработка персональных данных законодательно предусматривает поручение обработки персональных данных другому оператору (юридическому лицу), то с данным оператором заключается договор (соглашение), существенным условием которого является обязанность обеспечения указанным оператором конфиденциальности и безопасности персональных данных при их обработке.

5.3. Обработка персональных данных в Учреждении осуществляется:

- с согласия субъекта персональных данных, выраженного в письменной форме. Форма согласия на обработку персональных данных утверждена приказом директором Учреждения;

- на основании федеральных законов и нормативных актов, устанавливающих цель обработки персональных данных, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке.

5.4. При обработке персональных данных обеспечивается соблюдение конфиденциальности персональных данных и обеспечение необходимого уровня защиты информации. Данное требование обязательно для всех сотрудников и руководителей структурных подразделений Учреждения, руководителей Учреждения, осуществляющих обработку персональных данных.

6. Сведения, относящиеся к персональным данным, категории персональных данных

6.1. В Учреждении обрабатываются сведения, относящиеся к персональным данным:

- анкета;
- автобиография;
- образование;
- сведения о месте работы;
- сведения о составе семьи;

- паспортные данные;
- сведения о структурно-функциональном типе семьи;
- сведения о доходах получателя социальных услуг (членов его семьи);
- сведения о социальных льготах;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- содержание консультации;
- причина обращения гражданина;
- карты приема/план (программа) реабилитации получателя социальных услуг;
- личные дела получателей социальных услуг и документы, входящие в их состав, также сведения, содержащиеся в личных делах;
- фотографии и иные сведения, относящиеся к персональным данным получателя социальных услуг;
- рекомендации, характеристики получателя социальных услуг;
- другие сведения о получателях социальных услуг, полученные в ходе выполнения трудовых функций специалистов учреждения.

6.2. Учреждение осуществляет обработку следующих категорий персональных данных: фамилия, имя, отчество, год, месяц, дата рождения, место рождения, адрес, телефон, семейное положение, социальное положение, доходы, номер страхового свидетельства государственного пенсионного страхования, сведения о документах, удостоверяющих личность, не содержащие сведений о национальной принадлежности субъекта персональных данных.

7. Обязанности Учреждения при обработке персональных данных

7.1. При обработке персональных данных Учреждение обязано выполнять требования статей 18, 19, 20 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных" в том числе:

- безвозмездно предоставлять субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что обрабатываемые персональные данные, которые относятся к соответствующему субъекту, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и предпринятых мерах Учреждение обязано уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы;

- в случае выявления правонарушений с персональными данными Учреждение в срок, не превышающий трех рабочих дней с даты такого выявления, обязано устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений Учреждение в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязано уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение обязано уведомить субъекта персональных данных или его законного представителя;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Учреждение обязано прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных Учреждение обязано уведомить субъекта

персональных данных;

- обеспечивать конфиденциальность персональных данных, а именно:
- определить перечень персональных данных;
- определить перечень ответственных лиц;
- определить места хранения персональных данных;
- разработать систему нормативных документов, регламентирующих обработку персональных данных (в том числе с применением средств защиты информации);
- довести требования нормативных документов, регламентирующих обработку персональных данных, до сотрудников, обеспечивающих их обработку;
- закрепить ответственность сотрудников, обеспечивающих обработку персональных данных, по выполнению требований нормативных документов в их должностных инструкциях.

7.2. Обеспечивать конфиденциальность персональных данных не требуется:

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

8. Обязанности сотрудников Учреждения при работе с персональными данными и при обеспечении конфиденциальности и безопасности обработки персональных данных

8.1. Персональные данные являются одной из категорий Перечня сведений ограниченного доступа, не содержащих государственной тайны, и подлежат защите в рамках функционирующей в Учреждении системы защиты информации.

8.2. Сотрудники Учреждения при работе с персональными данными, при обеспечении их конфиденциальности и безопасности обработки обязаны выполнять весь комплекс мероприятий, установленный нормативными документами по обеспечению защиты информации, которые определяют правила работы:

- в системе защиты от несанкционированного доступа;
- при обеспечении антивирусной защиты;
- в системе криптографической защиты.

8.3. Общие правила:

- не сообщать персональные данные устно или письменно (по телефону, факсу, электронной почте, в письме или иным способом) кому бы то ни было, если это не установлено законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан;
- использовать учтенные (должным образом зарегистрированные) носители информации;
- не оставлять носители информации с персональными данными без присмотра или передавать на хранение другим лицам, не имеющим на это полномочий;
- выносить съемные носители информации, средства вычислительной техники с размещенными на них персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т.д.

9. Предоставление доступа к персональным данным

9.1. К работе с персональными данными допускаются сотрудники Учреждения, должностные инструкции которых предусматривают выполнение обязанностей по обработке персональных данных. Список лиц, имеющих доступ к персональным данным, утверждается директором Учреждения.

9.2. Предоставление сотруднику доступа к информационному ресурсу, содержащему персональные данные, осуществляется на основании приказа по Учреждению об утверждении списка лиц, осуществляющих обработку персональных данных по заявке (установленной формы) руководителя структурного подразделения Учреждения на имя директора Учреждения, с обоснованием необходимости работы с информационным ресурсом, режима работы в рамках функционирующей системы разграничения доступа.

9.3. Руководитель структурного подразделения Учреждения при организации доступа сотрудника к персональным данным, обязан ознакомить его с настоящим Порядком, с требованиями нормативных документов по установлению особенностей и правил осуществления обработки персональных данных, обеспечению безопасности персональных данных под роспись.

9.4. Каждый пользователь информационного ресурса имеет индивидуальные код (идентификатор) и пароль для доступа к информационному ресурсу. Пользователь не имеет права передавать свои учетные данные другому пользователю и несет персональную ответственность за конфиденциальность данных собственной учетной записи.

10. Обработка персональных данных

10.1. Обработка персональных данных в Учреждении осуществляется в соответствии с Положением по обработке персональных данных получателей социальных услуг в ГБУ «Комплексный центр социального обслуживания населения «Мыза» Приокского района города Нижнего Новгорода».

10.2. Обработка персональных данных осуществляется в Учреждении на основании действующего законодательства Российской Федерации, в соответствии с утвержденными инструкциями по обеспечению выполнения того или иного процесса в зависимости от цели обработки персональных данных (персонифицированный учет, предоставление социальных услуги т.д.).

11. Организация защиты персональных данных

11.1. Обработка персональных данных осуществляется с обеспечением необходимого уровня защиты информации, предусматривающего принятие организационных и технических мер, в том числе использование шифровальных (криптографических) средств, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

11.2. Обеспечение защиты персональных данных в Учреждении является одним из аспектов обеспечения защиты сведений ограниченного доступа, не составляющих государственную тайну, и осуществляется в рамках реализации комплексной системы защиты информации.

11.3. При обработке персональных данных с использованием средств автоматизации в Учреждении технические мероприятия выполняются в рамках реализации комплексной системы защиты информации и предусматривают:

- использование защищенной корпоративной информационно-телекоммуникационной сети;
- применение электронной цифровой подписи и шифрования данных при передаче;
- аутентификация пользователей вычислительных средств и информационных ресурсов;
- резервное копирование данных;
- авторизация доступа к информации;

- применение сертифицированных межсетевых защитных (фильтрующих) экранов;
- использование протоколов, обеспечивающих маршрутизацию сообщений;
- применение антивирусного мониторинга и детектирования;
- мониторинг процессов и действий пользователей аппаратных и информационных ресурсов;
- оборудование зданий и помещений системами пожарной и охранной сигнализации;
- применение для хранения парольной и ключевой информации электронных носителей (индивидуальных аутентификаторов, электронных ключей);
- применение в архитектуре вычислительных систем технологий и средств повышения надежности их функционирования и обеспечения безопасности информации;
- своевременное применение критических обновлений общесистемного и прикладного программного обеспечения;
- оптимальная настройка операционной системы и прикладного программного обеспечения (техническая и эксплуатационная документация на ППО).

12. Ответственность за нарушение требований обработки персональных данных

12.1 Нарушение требований обработки персональных данных, устанавливаемых законодательством Российской Федерации, нормативных документов по обеспечению безопасности сведений ограниченного доступа, не содержащих государственную тайну, и настоящим Положением, может повлечь гражданско-правовую, уголовную (в том числе по статьям Уголовного Кодекса Российской Федерации 137, 140, 272), административную (в том числе по статьям Кодекса об Административных Правонарушениях Российской Федерации 5.39, 13.11, 13.14), дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.