

ПОЛОЖЕНИЕ
о порядке обработки персональных данных в
Государственном бюджетном учреждении «Комплексный центр
социального обслуживания населения Уренского района»

I. Общие положения

1.1. Положение об обработке персональных данных в Государственном бюджетном учреждении «Комплексный центр социального обслуживания населения Уренского района» (далее - Положение) разработано в соответствии с частью 2 статьи 4 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Федеральный закон "О персональных данных"), Трудовым кодексом Российской Федерации, Постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", Постановлением Правительства Российской Федерации от 6 июля 2008 г. N 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 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

1.2. Положение определяет порядок и условия обработки персональных данных в Государственном бюджетном учреждении «Комплексный центр социального обслуживания населения Уренского района» (далее - Центр) с использованием средств автоматизации и без использования таких средств.

1.3. Обработка персональных данных в Центре осуществляется в целях исполнения требований законодательства Российской Федерации в области персональных данных, а также ведения кадровой работы (ведение и хранение личных дел, карточек и трудовых книжек работников) Центра, в целях обеспечения сохранности имущества Центра, документов, а также в целях предоставления социальных услуг, предоставление которых входит в полномочия Центра.

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

II. Порядок обработки персональных данных работников Центра и иных лиц

2.1. 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.

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

2.3. При обработке персональных данных в Центре организационные мероприятия выполняются в рамках реализации комплексной системы защиты информации и предусматривают:

- определение ответственных за обработку персональных данных и закрепление обязанностей и ответственности (издание приказа об утверждении списка сотрудников Центра, ответственных за обработку персональных данных, с возложением на них персональной ответственности за соблюдение порядка обработки и требований по защите персональных данных);
- информирование сотрудников, осуществляющих обработку персональных данных, о факте обработки ими персональных данных, категориях обрабатываемых персональных данных;
- ознакомление сотрудников, ответственных за обработку персональных данных, с требованиями нормативных документов по установлению особенностей и правил осуществления обработки персональных данных, обеспечению безопасности персональных данных под роспись;
- организация допуска и разграничение прав доступа к информационным ресурсам и материальным носителям, содержащим персональные данные, в рамках установленной системы разграничения доступа (подготовка разрешительных документов - таблиц разграничения доступа, заявок на допуск к информационному ресурсу). Работа с персональными данными лиц, не включенных в разрешительные документы, не допускается;
- внесение изменений в должностные инструкции сотрудников, имеющих отношение к обработке персональных данных, в части дополнения положениями о необходимости и обязанности соблюдения Положения о персональных данных, Положения о порядке обработки персональных данных, а также требований по их защите;
- внесение изменений в должностные инструкции руководителей структурных подразделений Центра в части дополнения положениями о необходимости и обязанности осуществления контроля за соблюдением

сотрудниками структурного подразделения правил обработки персональных данных, а также требований по их защите;

- определение перечня помещений, в которых осуществляется обработка информации, содержащей сведения ограниченного доступа, в т.ч. персональные данные;

- учет и контроль перемещения носителей информации, содержащих сведения ограниченного доступа, в т.ч. персональные данные.

2.4. Обработка персональных данных осуществляется как с использованием средств автоматизации, так и без использования таких средств.

2.5. При обработке персональных данных работников в целях реализации возложенных на Центр полномочий уполномоченные должностные лица обязаны соблюдать следующие требования:

- а) объем и характер обрабатываемых персональных данных, способы обработки персональных данных должны соответствовать целям обработки персональных данных;

- б) защита персональных данных работника от неправомерного их использования или уничтожения обеспечивается в порядке, установленном нормативными правовыми актами Российской Федерации;

- в) передача персональных данных работника не допускается без письменного согласия работника, за исключением случаев, установленных федеральными законами. В случае, если лицо, обратившееся с запросом, не обладает соответствующими полномочиями на получение персональных данных работника, либо отсутствует письменное согласие работника на передачу его персональных данных, Центр вправе отказать в предоставлении персональных данных. В этом случае лицу, обратившемуся с запросом, направляется письменный мотивированный отказ в предоставлении запрашиваемой информации;

г) обеспечение конфиденциальности персональных данных работников, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

д) хранение персональных данных должно осуществляться в форме, позволяющей определить работника и иное лицо, являющееся субъектом персональных данных, не дольше, чем этого требуют цели их обработки. Указанные сведения подлежат уничтожению по достижении цели обработки или в случае утраты необходимости в их достижении, если иное не установлено законодательством Российской Федерации. Факт уничтожения персональных данных оформляется соответствующим актом;

е) опубликование и распространение персональных данных работника допускается в случаях, установленных законодательством Российской Федерации.

2.6. Обработка биометрических и специальных категорий персональных данных работника или иного лица, являющегося субъектом персональных данных, осуществляется с их письменного согласия, за исключением случаев, предусмотренных законодательством Российской Федерации в области персональных данных. Использование и хранение биометрических и специальных категорий персональных данных вне информационных систем персональных данных может осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения.

2.7. В целях обеспечения защиты персональных данных субъект персональных данных вправе:

- самостоятельно принимать решение о предоставлении своих персональных данных и давать согласие на их обработку. При этом согласие на обработку персональных данных оформляется в письменном виде по рекомендуемой форме, утвержденной приказом Центра;

- отозвать согласие на обработку персональных данных путем направления письменного заявления на имя руководителя Центра;
- на получение сведений об операторе, о месте его нахождения, о наличии у оператора персональных данных, относящихся к соответствующему субъекту персональных данных, а также на ознакомление с такими персональными данными;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- на получение доступа к своим персональным данным лично или через законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе и собственноручную подпись субъекта персональных данных или его законного представителя. Запрос может быть представлен в электронной форме и подписан электронной цифровой подписью в соответствии с законодательством Российской Федерации;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке;
- обратиться с жалобой в уполномоченный федеральный орган исполнительной власти по защите прав субъектов персональных данных или в суд в том случае, если полагает, что обработка его персональных данных осуществляется с нарушением требований законодательства или иным образом нарушает его права и свободы.

2.8. Обязанности работников Центра при работе с персональными данными и при обеспечении конфиденциальности и безопасности обработки персональных данных:

- 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.

III. Порядок обработки персональных данных субъектов персональных данных, осуществляемой без использования средств автоматизации

3.1. При обработке персональных данных без использования средств автоматизации уполномоченными должностными лицами не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы.

3.2. При разработке и использовании типовых форм документов, необходимых для реализации возложенных на Центр полномочий, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), 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 обработки персональных данных, осуществляемой без использования средств автоматизации, адрес Центра, фамилию, имя, отчество и адрес

субъекта персональных данных, чьи персональные данные вносятся в указанную типовую форму, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, при необходимости получения согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов, чьи персональные данные содержатся в типовой форме, при ознакомлении со своими персональными данными, не имел возможности доступа к персональным данным иных лиц, содержащимся в указанной типовой форме;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.3. Уничтожение или обезличивание персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.4. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем изготовления нового материального носителя с уточненными персональными данными.

IV. Порядок обработки персональных данных субъектов персональных данных в информационных системах

4.1. Обработка персональных данных в Центре осуществляется:

- а) в Информационной системе "1С: Предприятие 8.3", включающей:
- фамилию, имя, отчество субъекта персональных данных;
 - дату рождения субъекта персональных данных;
 - серию и номер основного документа, удостоверяющего личность субъекта персональных данных;
 - сведения о дате выдачи указанного документа и выдавшем его органе;
 - адрес места жительства субъекта персональных данных;
 - почтовый адрес субъекта персональных данных;
 - ИНН субъекта персональных данных;
 - должность субъекта персональных данных;
 - номер приказа и дату приема на работу (увольнения) субъекта персональных данных;
 - номер страхового свидетельства государственного пенсионного страхования субъекта персональных данных;
 - гражданство субъекта персональных данных.

б) в Информационной системе "1С: Предприятие Зарплата + Кадры", включающей:

- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- серию и номер основного документа, удостоверяющего личность субъекта персональных данных;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- адрес места жительства субъекта персональных данных;
- почтовый адрес субъекта персональных данных;
- ИНН субъекта персональных данных;
- должность субъекта персональных данных;
- номер приказа и дату приема на работу (увольнения) субъекта персональных данных;
- номер страхового свидетельства государственного пенсионного страхования субъекта персональных данных;

- гражданство субъекта персональных данных.

в) в Информационной системе комплекс «СОЦПОМОЩЬ» включающей:

- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- серию и номер основного документа, удостоверяющего личность субъекта персональных данных;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- адрес места жительства субъекта персональных данных;
- СНИЛС субъекта персональных данных;
- семейное положение субъекта персональных данных;
- имущественное положение субъекта персональных данных;
- профессия субъекта персональных данных;
- доходы членов семьи субъекта персональных данных;
- льготы субъекта персональных данных;
- персональные данные о членах семьи субъекта персональных данных (паспортные данные, СНИЛС);
- реквизиты личного дела, договора и плата за обслуживание субъекта персональных данных.

г) в Информационной системе «ViP Net Деловая почта» включающей:

- фамилию, имя, отчество субъекта персональных данных;
- дату рождения субъекта персональных данных;
- адрес места жительства субъекта персональных данных.

Также информационная система «ViP Net Деловая почта» используется:

- для передачи конфиденциальной информации;
- для обновления комплекса «СОЦПОМОЩЬ»;
- для получения и использования ключей электронной подписи;
- для использования ЭЦП.

д) в Информационной системе «Регистр получателей социальных услуг Нижегородской области» включающей:

- фамилию, имя, отчество субъекта персональных данных;
- пол субъекта персональных данных;
- дату рождения субъекта персональных данных;
- возраст субъекта персональных данных;
- серию и номер основного документа, удостоверяющего личность субъекта персональных данных;
- сведения о дате выдачи указанного документа и выдавшем его органе;
- контактный телефон субъекта персональных данных;
- адрес места жительства (регистрации и фактический) субъекта персональных данных;
- социальный статус субъекта персональных данных;
- условия проживания субъекта персональных данных;
- заболевания субъекта персональных данных;
- СНИЛС субъекта персональных данных;
- трудоспособность субъекта персональных данных;
- награды и льготы субъекта персональных данных;
- реквизиты свидетельства о смерти субъекта персональных данных (указываются в случае смерти).

Также в информационной системе «Регистр получателей социальных услуг Нижегородской области» указываются оказанные социальные услуги субъекту персональных данных.

Центром используется информационная система «Реестр поставщиков социальных услуг Нижегородской области» содержащая следующую информацию:

- регистрационный номер учетной записи;
- полное и сокращенное наименование поставщика социальных услуг;
- дата государственной регистрации юридического лица, являющегося поставщиком социальных услуг;

- организационно-правовая форма поставщика социальных услуг (для юридических лиц);
- адрес (место нахождения, место предоставления социальных услуг), контактный телефон, адрес электронной почты поставщика социальных услуг;
- фамилия, имя, отчество руководителя поставщика социальных услуг;
- информация о лицензиях, имеющихся у поставщика социальных услуг (при необходимости);
- сведения о формах социального обслуживания;
- перечень предоставляемых социальных услуг по формам социального обслуживания и видам социальных услуг;
- тарифы на предоставляемые социальные услуги по формам социального обслуживания и видам социальных услуг;
- информация об общем количестве мест, предназначенных для предоставления социальных услуг, о наличии свободных мест, в том числе по формам социального обслуживания;
- информация об условиях предоставления социальных услуг;
- информация о результатах проведенных проверок;
- информация об опыте работы поставщика социальных услуг за последние пять лет.

Классификация указанных информационных систем персональных данных осуществляется в порядке, установленном законодательством Российской Федерации.

4.2. Персональные данные могут быть представлены для ознакомления:

а) сотрудникам, допущенным к обработке персональных данных с использованием средств автоматизации в части, касающейся исполнения их должностных обязанностей;

б) уполномоченным работникам федеральных органов исполнительной власти в порядке, установленном законодательством Российской Федерации.

4.3. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным.

4.4. Уполномоченными должностными лицами при обработке персональных данных в информационных системах персональных данных должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

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

4.6. Самостоятельное подключение средств вычислительной техники, применяемых для хранения, обработки или передачи персональных данных к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к информационно-телекоммуникационной сети Интернет, не допускается.

4.7. Доступ пользователей (операторов информационной системы) к персональным данным в информационных системах персональных данных Центра должен требовать обязательного прохождения процедуры идентификации и аутентификации.

4.8. Структурными подразделениями (должностными лицами) Центра, ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

а) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства Центра;

- б) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- в) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- г) постоянный контроль за обеспечением уровня защищенности персональных данных;
- д) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
- ж) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;
- з) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

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

- использование защищенного канала для передачи данных «ViP Net Деловая почта»;

- применение ключей 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 антивирусной защиты;
- 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 обновлений общесистемного и прикладного программного обеспечения;
- оптимальная настройка операционной системы и прикладного программного обеспечения.

4.10. В случае выявления нарушений порядка обработки персональных данных в информационных системах Центра уполномоченными должностными лицами принимаются меры по установлению причин нарушений и их устранению.

V. Ответственность за нарушение требований обработки персональных данных

5.1. 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.

VI. Заключительные положения

6.1. Настоящее Положение вступает в силу с 01 марта 2016 года.