



C=RU, O=ГБУ ЦППМСП
м.р.Кинель-Черкасский,
CN=Сибарцева А_А_,
E=ppms-kch@samara.edu.ru
00 8b 8d 8b 39 0c f7 10 80
2021-07-02 13:30:26

«УТВЕРЖДАЮ»

Директор ГБУ ЦППМСП

м.р. Кинель-Черкасский

Н.В. Комардина

Приказ № 19-од от 26.04.2016 года



ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ И ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

в государственном бюджетном учреждении – центр психолого-педагогической, медицинской и социальной помощи муниципального района Кинель-Черкасский Самарской области

Содержание

1. Общие положения.....	3
2. Понятие и состав персональных данных.....	4
3. Общие требования при обработке персональных данных.....	9
4. Принципы обработки персональных данных.....	10
5. Условия обработки персональных данных.....	11
6. Сбор накопление и систематизация персональных данных.....	13
7. Обработка персональных данных.....	20
8. Меры по обеспечению безопасности персональных данных при их обработке.....	23
9. Доступ к персональным данным.....	25
10. Защита персональных данных.....	27
11.Права и обязанности субъекта персональных данных.....	32
12.Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.....	33

1. Общие положения

1.1. Положение об обработке и защите персональных данных в государственном бюджетном учреждении – центр психолого-педагогической, медицинской и социальной помощи м.р. Кинель-Черкасский Самарской области (далее - Учреждение) регулирует отношения, связанные с обработкой персональных данных, осуществляемой лицами, уполномоченными на получение, обработку, хранение, передачу и другое использование персональных данных с использованием средств автоматизации или без использования таких средств.

1.2. Целью данного Положения является защита персональных данных в Учреждении от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Настоящее Положение разработано на основании статей 24 Конституции РФ, главой 14 Трудового Кодекса РФ, Федерального закона «Об информации, информатизации и защите информации» от 27.07.2006 г. № 149-ФЗ, Федерального закона «О защите персональных данных» от 27.07.2006 г. № 152-ФЗ, Федерального закона «О внесении изменений в Федеральный закон «О защите персональных данных» от 25.07.2011 № 261-ФЗ, Приказа ФСТЭК России от 18.02.2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных», Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях», от 21.07.2014, № 242-ФЗ, Постановление правительства РФ от 15 сентября 2008г. № 687 «Об утверждении Положения

об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, и других нормативных документов.

1.4. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

1.5. Настоящее Положение определяет порядок работы (сбор, обработка, хранения передача и т. д.) с персональными данными субъектов и гарантии конфиденциальности сведений о субъекте, предоставленных оператору, утверждается и вводится в действие приказом директора и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным.

2. Понятие и состав персональных данных

2.1. В настоящем положении используются следующие основные понятия:

1) **Персональные данные** – любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)

2) **Субъект-субъект персональных данных.**

К субъектам персональных данных в ГБУ ЦППМСП м.р. Кинель-Черкасский далее – (субъекты) относятся лица – носители персональных данных, передавшие свои персональные данные в ГБУ ЦППМСП м.р. Кинель-Черкасский (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для приема, получения, поиска, сбора, систематизации, накопления, хранения, уточнения, обновления,

изменения, использования, распространения (в том числе передачи), обезличивания, в том числе:

- работники Учреждения

- иные лица, предоставляющие персональные данные в Учреждение;

3) **Работник** – Физическое лицо, вступившее в трудовые отношения с ГБУ ЦППМСП м.р. Кинель-Черкасский;

4) **Иное лицо** – физическое лицо, состоящее в договорных отношениях и иных гражданско-правовых отношениях с ГБУ ЦППМСП м.р. Кинель-Черкасский;

5) **Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

6) **Обработка персональных данных** - 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;

7) **Сбор персональных данных** – накопление информации на материальных носителях и (или) в автоматизированных системах;

8) **Накопление и систематизирование персональных данных** – организация размещения персональных данных, которое обеспечивает быстрый поиск и отбор нужных сведений, методическое обновление данных, защиту их от искажений, потери;

9) **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

10) **Хранение персональных данных** - комплекс мероприятий, направленный на обеспечение сохранности полноты и целостности сформированных массивов персональных данных, создание и поддержание надлежащих условий для их использования, а также предупреждение несанкционированного доступа, распространения и использования;

11) **Уточнение персональных данных** - процесс поддержания персональных данных в актуальном состоянии;

12) **Доступ к персональным данным** - возможность получения персональных данных и их использования;

13) **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

14) **Конфиденциальность персональных данных** – обязательное для соблюдения лицом, уполномоченным на получение, обработку, хранение, передачу и другое использование персональных данных или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

15) **Распространение персональных данных** - действия, направленные на раскрытие персональных данных определенному кругу лиц;

16) **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

17) **Уничтожение персональных данных** - действия, в результате которых становится невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

18) **Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

19) **Информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

20) **Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.2. В состав персональных данных субъекта входят:

- фамилия, имя, отчество;
- год, месяц, число и место рождения;
- гражданство;
- сведения о знании иностранных языков;
- документы, удостоверяющие личность, паспорт (номер, серия, дата выдачи, кем выдан, код подразделения);
- идентификационный номер налогоплательщика;
- номер и серия страхового свидетельства государственного пенсионного страхования;
- адреса фактического места проживания и регистрации по месту жительства, дата регистрации по месту жительства;
- почтовые и электронные адреса;
- номера телефонов (сотовый, домашний);
- фотографии;
- сведения об образовании (наименование учебного заведения, год окончания, документ об образовании, квалификация, специальность);
- сведения о профессии, стаже работы (общий, непрерывный, дающий право на выслугу лет) и занимаемых ранее должностях;

- сведения о семейном положении и составе семьи (степень родства (ближайшие родственники, ФИО родственников, год их рождения);
- сведения о воинском учете;
- сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и наказаниях, почетных званиях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.);
- сведения о состоянии здоровья, необходимые работодателю для определения пригодности для выполнения поручаемой работы и предупреждения профессиональных заболеваний, предусмотренные действующим законодательством Российской Федерации;
- сведения о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора;
- сведения об отсутствии судимости;
- сведения о заработной плате работника;
- подлинники и копии приказов по личному составу, основания к ним;
- дополнительные сведения, представленные мною по собственному желанию и другие персональные данные, необходимые работодателю в соответствии с действующим законодательством Российской Федерации в области персональных данных.

2.3. Указанные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

2.4. Ответственные лица за обеспечение безопасности персональных данных и лица, уполномоченные на получение, обработку, хранение, передачу и другое использование персональных данных обеспечивают защиту персональных данных работников и иных лиц, содержащихся в их

личных делах и иных документах, в автоматизированных информационных системах персональных данных (далее – ИСПДн) от неправомерного их использования или утраты. Приказом директора центра назначается ответственное лицо за обеспечение безопасности персональных данных в организации.

3. Общие требования при обработке персональных данных

3.1. Лица, уполномоченные на получение, обработку, хранение, передачу и другое использование персональных данных при обработке персональных данных субъекта персональных данных, обязаны соблюдать следующие общие требования:

3.1.1. Обработка персональных данных субъекта персональных данных может осуществляться исключительно в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов, исполнения трудового и гражданско-правового договоров, содействия субъекту персональных данных в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности субъекта персональных данных, контроля количества и качества выполняемой работы, качества освоения образовательных программ и обеспечения сохранности имущества Учреждения и субъекта персональных данных.

3.1.2. Все персональные данные субъекта персональных данных следует получать у него самого в устной форме, либо в письменной форме путем заполнения различных анкет, опросных листов и т.п. Если персональные данные субъекта персональных данных возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие (либо письменный отказ) (Приложение № 3). Лицо, уполномоченное на получение, обработку, хранение, передачу и другое

использование персональных данных, должно сообщить субъекту персональных данных о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта персональных данных дать письменное согласие на их получение.

3.1.3. Обработка персональных данных субъекта персональных данных о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, личной или интимной жизни, о его членстве в общественных объединениях или его профсоюзной деятельности не допускается, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации и иными федеральными законами.

3.1.4. При принятии решений, затрагивающих интересы субъекта персональных данных недопустимо основываться на персональные данные, полученные исключительно в результате их автоматизированной обработки или электронного получения.

4. Принципы обработки персональных данных

4.1. Принципы обработки персональных данных:

1) Обработка персональных данных должна осуществляться на законной и справедливой основе.

2) Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3) Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4) Обработке подлежат только персональные данные, которые отвечают целям их обработки.

5) Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

6) При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

7) Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Условия обработки персональных данных.

5.1. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным законом «О защите персональных данных». Обработка персональных данных допускается в следующих случаях:

1) обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

2) обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения, возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;

3) обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);

4) обработка персональных данных необходима для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", для обеспечения предоставления такой услуги, для регистрации субъекта персональных данных на едином портале государственных и муниципальных услуг;

5) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

6) обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

7) обработка персональных данных осуществляется в статистических или иных исследовательских целях, при условии обязательного обезличивания персональных данных;

8) осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных);

9) осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

3.2.3. Особенности обработки специальных категорий персональных данных, а также биометрических персональных данных устанавливаются соответственно статьями 10 и 11 Федерального закона № 152-ФЗ.

6. Сбор, накопление и систематизация персональных данных.

6.1. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом. В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 ФЗ № 152.

6.2. Лицо, осуществляющее обработку персональных данных по поручению оператора, не обязано получать согласие субъекта персональных данных на обработку его персональных данных.

6.3. В случае если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

6.4. Конфиденциальность персональных данных.

6.4.1. Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6.5. Общедоступные источники персональных данных.

6.5.1. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных.

6.5.2. Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

6.6. Согласие субъекта персональных данных на обработку своих персональных данных.

6.6.1. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе (Приложение 1). Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его

представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются оператором.

6.6.2. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных (Приложение 2). В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152 от 27.07.2006 года.

6.6.3 Обязанность представить доказательство получения согласия субъекта персональных данных на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона № 152 от 27.07.2006 года, возлагается на оператора.

6.6.4. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

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

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных).

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

6.6.5. Порядок получения в форме электронного документа согласия субъекта персональных данных на обработку его персональных данных в целях предоставления государственных и муниципальных услуг, а также услуг, которые являются необходимыми и обязательными для предоставления государственных и муниципальных услуг, устанавливается Правительством Российской Федерации.

6.6.6. В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает законный представитель субъекта персональных данных. (Приложение 3)

6.6.7. В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни.

6.6.8. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 ФЗ № 152.

6.7. Сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (биометрические персональные данные), могут получаться и обрабатываться только при наличии согласия субъекта персональных данных в письменной форме. Обработка биометрических персональных данных может осуществляться без согласия субъекта в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, уголовно-исполнительным законодательством Российской Федерации.

6.8. Специальная категория персональных данных это данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной, частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, Оператор не имеет права получать и обрабатывать специальную категорию персональных данных, за исключением, если:

- субъект дал согласие в письменной форме на обработку своих соответствующих персональных данных;
- персональные данные являются общедоступными;

- персональные данные относятся к состоянию здоровья субъекта и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц, и получение согласия субъекта в данный момент невозможно;
- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
- обработка персональных данных необходима в связи с осуществлением правосудия;
- обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст.24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия.

Обработка персональных данных, перечисленных в п.3.7 настоящего Положения, должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась обработка.

6.9. Так же согласие субъекта на получение и обработку его персональных данных не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

- обработка персональных данных осуществляется в целях исполнения трудового или иного договора или соглашения между работником и оператором;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта, если получение его согласия при данных обстоятельствах невозможно;

- обработка персональных данных необходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами.

6.10. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, электронные базы). В общедоступные источники персональных данных с письменного согласия работника могут включаться его фамилия, имя, отчество, год и место рождения, адрес, сведения о профессии и иные персональные данные, предоставленные работником.

6.11. Персональные данные работников обрабатываются с использованием автоматизированных систем:

- ИСПДн ПП «Кластер:Бюджет»-Бухгалтерия;
- ИСПДн Сбербанк – Онлайн;
- ИСПДн «Кадры»;
- ИСПДн «УРМ: Бюджет»;
- ИСПДн «Контур-Экстерн».

7. Обработка персональных данных

7.1. Под обработкой персональных данных субъекта понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных.

7.2. В целях обеспечения прав и свобод человека и гражданина оператор и его представители при обработке персональных данных обязаны соблюдать следующие общие требования:

7.2.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия субъектам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

7.2.2. При определении объема и содержания, обрабатываемых персональных данных субъекта, оператор должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

7.2.3. Получение персональных данных может осуществляться как путем представления их самим субъектом, так и путем получения их из иных источников.

7.2.4. Если персональные данные субъекта можно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

7.2.5. Оператор не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и

частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны только с его письменного согласия.

7.2.6. Оператор не имеет право получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

7.3. К получению, обработке, передаче и хранению персональных данных субъекта могут иметь доступ:

- работники администрации Учреждения;
- работники бухгалтерского учета Учреждения;
- представители органов управления образования муниципального, регионального и федерального уровней;
- иные работники Учреждения (работа с персональными данными субъектов в части их касающейся).

7.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

7.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

7.5. Передача персональных данных субъекта возможна только с его согласия или в случаях, прямо предусмотренных законодательством.

7.5.1. При передаче персональных данных оператор должен соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные субъекта, 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 субъекта, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья субъектов, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции, сведений необходимых для выполнения трудовых обязанностей.
- передавать персональные данные субъектов представителям субъектов в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными, субъектов которые необходимы для выполнения указанными представителями их функций.

7.5.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

7.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных субъектов распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

7.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

7.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

7.9. Конкретные обязанности по хранению сведений о субъектах персональных данных, заполнению, хранению и выдаче документов, ведению информационной базы персональных данных отражающих персональные данные, возлагаются на работников Учреждения и закрепляются в должностных инструкциях. Так же назначаются ответственные за организацию обработки персональных данных приказом директора.

8. Меры по обеспечению безопасности персональных данных при их обработке

8.1. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

8.2. Обеспечение безопасности персональных данных достигается, в частности:

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 Российской Федерации уровни защищенности персональных данных;

3) применением прошедших в установленном порядке процедуру оценки 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 данным 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 над принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

10) использование и хранение биометрических персональных данных вне информационных систем персональных данных могут 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, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

11) под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

9. Доступ к персональным данным

9.1 Внутренний доступ к персональным данным без специального разрешения имеют работники, занимающие в организации следующие должности (только в пределах своей компетенции):

- директор учреждения;
- заместитель директора;
- работники бухгалтерии;
- работник секретариата (информация о фактическом месте проживания, контактные телефоны субъектов и др.);
- инженер (информация о фактическом месте проживания и контактные телефоны субъектов и др.);
- инженер-программист (информация в информационных базах);
- методист, психолог (доступ к персональным данным в части его касающейся) (Приложение 4);
- сам субъект персональных данных.

9.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом руководителя.

9.2. Внешний доступ.

9.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных и государственных органов управления;

9.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

9.2.3. Организации, в которые работник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

9.3. Другие организации.

Сведения о работающем или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта.

В случае развода бывшая супруга (супруг) имеют право обратиться в организацию с письменным запросом о размере заработной платы работника без его согласия. (УК РФ).

9.4. Работник Учреждения имеет право:

9.4.1. Получать доступ к своим персональным данным и знакомиться с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные работника.

9.4.2. Требовать от Работодателя уточнения, блокирования или уничтожения неполных, недостоверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Работодателя персональных данных.

9.4.3. Получать от Работодателя

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

- перечень обрабатываемых персональных данных и источник их получения;

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

- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

9.4.4. Требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

10. Защита персональных данных

10.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

10.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные

обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

10.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

10.4. Защита персональных данных субъекта от неправомерного их использования или утраты должна быть обеспечена оператором за счет его средств в порядке, установленном федеральным законом.

10.5. «Внутренняя защита».

10.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

10.5.2. Для обеспечения внутренней защиты персональных данных субъектов необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно – правовых документов по защите информации и сохранении тайны;

- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находятся персональные данные субъектов;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с работниками управления по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места руководителей.
- в отсутствие работника, имеющего доступ к персональным данным, на его рабочем месте не должно быть документов, содержащих персональные данные субъектов. Уборка в кабинете ответственного лица проводится только в его присутствии. Размещение рабочего места исключает бесконтрольное использование данной информации.

10.5.3. При обработке персональных данных в информационных системах Учреждения обеспечивается следующее:

- а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- г) возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных

10.5.4. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

д) учет лиц, допущенных к работе с персональными данными в информационной системе;

и) 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;

к) описание системы защиты персональных данных.

10.6. Иные права, обязанности, действия работников определяются также должностными инструкциями работников, приказами и распоряжениями Директора ГБУ ЦППМСП м.р.Кинель-Черкасский, локальными нормативными актами ГБУ ЦППМСП м.р.Кинель-Черкасский.

10.7. «Внешняя защита».

10.7.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

10.7.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

10.7.3. Для обеспечения внешней защиты персональных данных необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

10.8. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников (Приложение 5, Приложение 6, Приложение 7).

10.9. По возможности персональные данные обезличиваются.

11. Права и обязанности субъекта персональных данных

11.1. В целях обеспечения защиты персональных данных, хранящихся в ГБУ ЦППМСП м.р. Кинель-Черкасский, субъект персональных данных имеет право на:

- полную информацию о своих персональных данных и обработке этих данных, в том числе автоматизированной;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом;
- определение своих представителей для защиты своих персональных данных;
- доступ к относящимся к нему медицинским данным с помощью медицинского специалиста по его выбору;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса Российской Федерации или иного федерального закона;
- требование об извещении всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия при обработке и защите его персональных данных;
- отзывать согласие на обработку персональных данных.

11.2. В целях обеспечения достоверности персональных данных субъект персональных данных обязан:

- предоставить полные достоверные данные о себе;
- в случае изменения сведений, составляющих персональные данные, незамедлительно известить оператора о соответствующих изменениях.

12. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными.

12.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

12.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

12.3. Руководитель, разрешающий доступ работника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

12.4. Каждый работник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

12.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

12.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

12.5.2. Должностные лица, в обязанность которых входит ведение персональных данных субъектов, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

12.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

12.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказываются штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

12.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.