

Приложение 1
к приказу
ГБУ СО КК
«Ейский КЦСОН»
от 30.12.2021 № 402

«Приложение 1

УТВЕРЖДЕНО
приказом ГБУ СО КК
«Ейский КЦСОН»
от 30.12.2021 г. № 402
(в редакции приказа
ГБУ СО КК
«Ейский КЦСОН»
от 30.12.2021 № 402)

ПОЛОЖЕНИЕ
о порядке обработки персональных данных
ГБУ СО КК «Ейский КЦСОН»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящим положением определяется порядок обращения с персональными данными в государственном бюджетном учреждении социального обслуживания Краснодарского края «Ейский комплексный центр социального обслуживания населения» (далее – Учреждение).

1.2 Упорядочение обращения с персональными данными имеет целью обеспечить соблюдение законных прав интересов Учреждения и субъектов персональных данных в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.

1.3 Персональные данные работника – любая информация, относящаяся к конкретному работнику (субъекту персональных данных) и необходимая Учреждению в связи с трудовыми отношениями.

1.4 Персональные данные гражданина - любая информация, относящаяся к конкретному гражданину (субъекту персональных данных) и необходимая Учреждению для осуществления своей деятельности.

1.5 Сведения о персональных данных субъектов персональных данных относятся к числу конфиденциальных (составляющих охраняемую законом тайну Учреждения). Режим конфиденциальности в отношении персональных данных снимается:

в случае их обезличивания;

в других случаях, предусмотренных федеральным законодательством РФ.

1.6 Цель разработки настоящего Положения является обеспечение защиты прав и свобод человека и гражданина, при обработке его персональных данных, в том числе права на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.7 Положение разработано в соответствии со следующими нормативными актами:

- 1) Конституцией Российской Федерации;
- 2) Гражданским кодексом Российской Федерации;
- 3) Кодексом об Административных правонарушениях РФ;
- 4) Трудовым кодексом Российской Федерации;
- 5) Федеральным законом от 27 июля 2006г. № 152-ФЗ «О персональных данных» (далее Федеральный закон № 152-ФЗ);
- 6) Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информатизации, информационных технологиях и о защите информации»;
- 7) Федеральным законом от 28 декабря 2013 года № 442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации»;
- 8) Постановлением Правительства Российской Федерации от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 9) Постановлением Правительства РФ от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 10) другими нормативно-правовыми актами Российской Федерации, относящиеся к вопросу обработки и защиты персональных данных;
- 11) договорами, заключаемыми между Оператором и субъектом персональных данных;
- 12) согласием на обработку, предоставление и распространение персональных данных субъектов персональных данных;
- 13) внутренними документами Оператора в области защиты персональных данных.

1.8 Положение определяет необходимый минимальный объем мер, соблюдение которых позволяет предотвратить утечку сведений, относящихся к персональным данным. При необходимости могут быть введены дополнительные меры, направленные на усиление защиты персональных данных.

2. Основные понятия и состав персональных данных

2.1 Для целей настоящего Положения используются следующие основные понятия:

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

безопасность персональных данных - состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

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 совершаемые с персональными данными;

несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному назначению и техническим характеристикам;

персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных) (п.1 ст.3 Федерального закона от 27 июля 2006 г. № 152-ФЗ);

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 (п. 3 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ);

распространение персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (п. 5 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ);

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ);

блокирование персональных данных - временное прекращение обработки персональных данных работников (за исключением случаев, если обра-

ботка необходима для уточнения персональных данных) (п.7 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ);

уничтожение персональных данных - действия, в результате которых становится невозможными восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников (п. 8 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ);

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику (п. 9 ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ);

информация - сведения (сообщения, данные) независимо от формы их представления;

документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу;

субъекты персональных данных - физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных, а именно работники учреждения и граждане, обратившиеся в учреждение.

2.2 Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 ТК РФ лицо, поступающее на работу предъявляет:

паспорт или иной документ, удостоверяющий личность;

трудовую книжку или сведения о трудовой деятельности, за исключением случаев, когда договор заключается впервые, или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой, повреждением или по другим причинам;

документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;

идентификационный номер налогоплательщика (ИНН);

документы воинского учета – для военнообязанных и лиц, подлежащих призыву на военную службу;

документ об образовании и (или) квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;

свидетельства о заключении (расторжении) брака;

свидетельства о рождении детей;

документы о праве на льготы (удостоверение почетного донора, справка о признании лица инвалидом и др. на усмотрение работодателя);

справку, выданную органами МВД России о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, к выполнению которой в соответствии с трудовым кодексом РФ или иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию) (п.п. 14,15 Административного регламента, утвержденного приказом МВД России от 7 ноября 2011 г. № 1121);

медицинское заключение по результатам прохождения предварительного медицинского осмотра.

2.3 При оформлении работника специалистом по кадрам заполняется унифицированная форма Т-2 «Личная карточка работника». После заключения трудового договора и издания приказа о приеме на работу формируется личное дело работника, в которое включаются документы и подшиваются в следующей последовательности:

личный листок по учету кадров, анкета, заполняется лично работником;

заявление о приеме на работу;

трудовой договор с работником;

копия (выписка) приказа о приеме на работу;

справка установленного образца о наличии (отсутствии) судимости;

согласие на обработку персональных данных;

обязательство о неразглашении персональных данных;

договор о материальной ответственности (для материально ответственных лиц).

В процессе ведения личного дела в него включаются документы, характеризующие деловые и личные качества работника:

характеристика и аттестационные листы;

копии документов о повышенной квалификации, профессиональной переподготовке;

заявление работника о переводе, увольнении, иные документы, послужившие основанием для перевода, увольнения работника;

копии (выписки) приказов о переводе, увольнении, награждении, изменении фамилии, присвоении квалификационных категорий, разрядов и т.п.

2.4 Специалисты по кадрам Учреждения создают и хранят следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

1) Документы, содержащие персональные данные работников:

комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;
подлинники и копии приказов (распоряжений) по кадрам;
личные дела и трудовые книжки;
дела, содержащие основания к приказу по личному составу;
дела, содержащие материалы внутренних расследований;
справочно-информационный банк данных по персоналу (картотеки, журналы);

подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений;

копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

2) документы по организации работы структурных подразделений:

положения о структурных подразделениях;

должностные инструкции работников;

документы планирования, учета, анализа и отчетности по вопросам кадровой работы.

2.5 Специалист по охране труда формирует и хранит списки работников Учреждения, направляемых на периодические медицинские осмотры, хранит медицинские книжки работников и медицинские заключения по результатам проведенных медицинских осмотров.

2.6 В состав персональных данных граждан, признанных нуждающимися в предоставлении социальных услуг, входят документы, содержащие информацию о фамилии, имени, отчестве, паспортных данных, контактных номерах телефонов, адресе проживания (регистрации), дате рождения, месте рождения, семейном положении, составе семьи, о доходах, СНИЛС, состоянии здоровья, о праве на льготы.

Информация, предоставляемая гражданином, признанным в установленном порядке, нуждающимся в предоставлении социальных услуг при обращении в Учреждение должна иметь документальную форму.

Специалисты по социальной работе выполняющие функции заведующего отделением надомного социального обслуживания, при приеме на социальное обслуживание формируют личное дело гражданина в соответствии с требованиями действующего законодательства.

2.7 В состав персональных данных граждан, обратившихся в учреждение за получением социальных услуг, входят документы, содержащие информацию о фамилии, имени, отчестве, паспортных данных, контактных номерах телефонов, адресе проживания (регистрации), дате рождения, месте рождения, семейном положении, о праве на льготы.

Информация, предоставляемая гражданином, обратившимся в Учреждение за предоставлением социальных услуг, должна иметь документальную форму.

Граждане, обратившиеся в учреждение за предоставлением социальных услуг при обращении в Учреждение должны иметь документы предусмотренные действующим законодательством РФ.

3. Обработка персональных данных

3.1 Источником информации обо всех персональных данных работника является непосредственно работник. Если персональные данные возможно получить только у третьей стороны, то работник должен быть заранее в письменной форме уведомлен об этом, и от него должно быть получено письменное согласие. Работодатель обязан сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о последствиях отказа работника дать письменное согласие на их получение.

3.2 Оператор не имеет права получать и обрабатывать персональные данные субъекта о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работников только с его письменного согласия.

3.3 Обработка персональных данных субъектов персональных данных работодателем возможна только с их согласия либо без их согласия в случаях предусмотренных действующим законодательством.

3.4 Оператор вправе обрабатывать персональные данные субъектов только с их письменного согласия.

3.5 Письменное согласие субъекта на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшего его органа;

- наименование (фамилию, имя, отчество) и адрес учреждения, получающего согласие субъекта персональных данных;

- цель обработки персональных данных;

- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

- срок, в течение которого действует согласие, а также порядок его отзыва.

3.6 Согласие субъекта не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные, которых подлежат обработке, а также определенного полномочия Оператора;

- обработка персональных данных в целях исполнения трудового договора;

- 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 невозможно.

3.7 Субъект персональных данных представляет уполномоченному работнику Учреждения достоверные сведения о себе.

3.8 В соответствии со ст. 86 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина руководитель Учреждения и его законные представители при обработке персональных данных работников должны выполнять следующие общие требования:

1) Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных правовых актов, содействия работникам в трудоустройстве, получения образования и профессиональном продвижении, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2) При определении объема и содержании обрабатываемых персональных данных работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

3) При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональные данные, полученные о нем исключительно в результате их автоматизированной обработки или электронного получения.

4) Защита персональных данных работника от неправомерного их использования, утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.

Во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

3.9 Персональные данные подлежат уничтожению либо обезличиванию в следующих случаях:

1) Достижение целей обработки или в случае утраты необходимости в их достижении.

2) Отзыва согласия субъекта персональных данных на обработку персональных данных.

3) Представления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

4) Выявление неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя и невозможности обеспечить правомерную обработку персональных данных.

3.10 Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются в соответствии со списком, утвержденным в порядке, определяемом в Учреждении.

3.11 В срок, не превышающий 7 дней со дня предоставления субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Учреждение вносит в них необходимые изменения, а также уведомляет субъекта о внесенных изменениях.

3.12 Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами Российской Федерации.

3.13 Уничтожение персональных данных осуществляется в срок, не превышающий 30 рабочих дней с момента отзыва согласия субъекта персональных данных на обработку персональных данных.

3.14 Уничтожение персональных данных осуществляется в срок, не превышающий 7 рабочих дней с момента представления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки.

3.15 В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его законного представителя и невозможности обеспечить правомерную обработку персональных данных уничтожение персональных данных осуществляется в срок, не превышающий 10 рабочих дней с момента выявления неправомерной обработки персональных данных. Решение о неправомерной обработке персональных данных и необходимости уничтожения персональных данных принимает ответственный за организацию обработки персональных данных, который доводит соответствующую информацию до руководства. Учреждение уведомляет субъекта персональных данных или его законного представителя об уничтожении персональных данных.

3.16 Уничтожение персональных данных осуществляет комиссия в составе работников структурного подразделения, обрабатывающего персональные данные субъекта и установившего необходимость уничтожения персональных данных под контролем руководителя этого структурного подразделения.

3.17 Способ уничтожения материальных носителей персональных данных определяется комиссией. Допускается применение следующих способов:

- 1) сжигание;
- 2) шредирование (измельчение);
- 3) передача на специализированные полигоны (свалки);
- 4) химическая обработка.

При этом составляется акт, подписываемый председателем комиссии, проводившей уничтожение материальных носителей персональных данных.

При необходимости уничтожения большого количества материальных носителей или применения специальных способов уничтожения допускается привлечение специализированных организаций. В этом случае комиссия Учреждения должна присутствовать при уничтожении материальных носителей

персональных данных. При этом к акту уничтожения необходимо приложить накладную на передачу материальных носителей персональных данных, подлежащих уничтожению, в специализированную организацию.

3.18 Уничтожение полей баз данных Учреждения, содержащих персональные данные субъекта, выполняется в случаях, установленных в п.3.9 по заявке руководителя структурного подразделения, обрабатывавшего персональные данные субъекта и установившего необходимость их уничтожения.

3.19 Уничтожение осуществляет комиссия, в состав которой входят лица, ответственные за техническое обслуживание автоматизированных систем, которым принадлежат базы данных.

3.20 Уничтожение достигается путем затирания информации на носителях информации (в том числе и резервных копиях). При этом составляется акт, утверждаемый лицом, ответственным за техническое обслуживание автоматизированных систем, которому принадлежат база данных.

3.21 Уничтожение архивов электронных документов и протоколов электронного взаимодействия может не производиться, если ведение и сохранность их в течение определенного срока предусмотрены соответствующими нормативными и (или) договорными документами.

3.22 При отсутствии технической возможности осуществить уничтожение персональных данных, содержащихся в базах данных, допускается проведение обезличивания путем перезаписи полей баз данных. Перезапись должна быть осуществлена таким образом, чтобы дальнейшая идентификация субъекта персональных данных была не возможна.

3.23 Контроль выполнения процедур уничтожения персональных данных осуществляет ответственный за организацию обработки персональных данных.

3.24 Обработка биометрических персональных данных (фотография, видео), используемая для идентификации в соответствии со ст.11 ФЗ № 152-ФЗ, допускается при наличии согласия субъекта персональных данных. Форма согласия утверждается приказом директора Учреждения. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкеты, бланки).

3.25 Решение, порождающие юридические последствия в отношении субъекта персональных данных или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме субъекта персональных.

3.26 Работники должны быть ознакомлены под подпись с настоящим Положением и другими документами Учреждения, устанавливающими порядок обработки персональных данных субъектов, а также права и обязанности в этой области.

4. Правила работы с обезличенными данными

4.1 Порядок обезличивания включает в себя замену идентифицирующей информации о субъекте (например: фамилию, имя и отчество на произвольный код (далее идентификатор).

4.2 Обезличивание должно проводиться таким образом, чтобы определить принадлежность персональных данных конкретному субъекту персональных данных было невозможно без использования дополнительной информации.

4.3 В случае, если обезличенные персональные данные используются в статистических или иных исследовательских целях, сроки обработки и хранения персональных данных устанавливаются руководством Учреждения исходя из служебной необходимости, и получение согласия субъекта на обработку его персональных данных на основании п.9 части 1 ст. 6 Федерального Закона № 152-ФЗ не требуется.

4.4 Если обезличенные персональные данные используются в целях продвижения услуг Учреждения, то получение согласия субъекта персональных данных обязательно.

4.5 Методы и способы защиты информации от несанкционированного доступа для обеспечения безопасности обезличенных персональных данных в информационных системах и целесообразность их применения определяются ответственным за организацию обработки персональных данных Учреждения индивидуально для каждой системы персональных данных.

5. Передача и хранение персональных данных

5.1 При передаче персональных данных субъекта персональных данных Оператором должен соблюдаться следующие требования:

1) Не сообщать персональные данные субъекта третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральным законом.

2) Не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия.

3) Предупредить лиц, получивших персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные субъекта, обязаны соблюдать режим секретности (конфиденциальности), данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральным законом.

4) Осуществлять передачу персональных данных субъектов в пределах Учреждения в соответствии с настоящим Положением.

5) Разрешать доступ к персональным данным субъектов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

6) Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

7) Передавать персональные данные субъекта его законным полномочным представителем в порядке, установленном Трудовым кодексом РФ, и ограничивать эту информацию только теми персональными данными.

5.2 Хранение материальных носителей персональных данных осуществляется в специально оборудованных шкафах и сейфах. Места хранения определяются в соответствии со списком, утвержденным в порядке, определенном в Учреждении.

5.3 Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

5.4 Получение персональных данных субъекта у третьих лиц, возможно только при уведомлении субъекта об этом заранее и с его письменного согласия. Форма согласия утверждается приказом директора Учреждения. Допускается совмещение формы согласия субъекта с типовыми формами документов, содержащих персональные данные субъекта (например: анкета, бланки, заявления).

5.5 Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше чем этого требуют цели их обработки.

6. Доступ к персональным данным

6.1 Право доступа к персональным данным работников имеют:

- 1) директор учреждения;
- 2) заместители директора;
- 3) начальник отдела кадров;
- 4) специалисты по кадрам;
- 5) делопроизводитель (доступ к персональным данным работников в ходе работы с документами архива);
- 6) специалист по социальной работе, выполняющий трудовые функции заведующего организационно-методическим отделением (далее – ОМО), специалисты по социальной работе ОМО (доступ к персональным данным, в том числе биометрических, в ходе плановых проверок и для осуществления мероприятий по повышению профессионального уровня работников, определения победителей конкурсов, при определении лучшего работника месяца, участия в семинарах);
- 7) заведующий складом (информация, необходимая при закупке средств индивидуальной защиты: Ф.И.О., размерный ряд одежды, обуви);
- 8) специалист по охране труда (информация, необходимая для прохождения медицинских осмотров, диспансеризации: Ф.И.О., дата рождения и др.);

9) программист (системный администратор системы персональных данных);

10) специалист по социальной работе, выполняющий трудовые функции заведующего отделением (доступ к персональным данным работников своего подразделения);

11) ведущий специалист ГО и ЧС (информация о фактическом месте проживания и контактные телефоны работников);

12) экономист (информация, необходимая для подготовки ежемесячного отчета о нагрузке социальных работников);

13) юрисконсульт (информация, необходимая для заключения договоров на, обучение, проведение предварительных и периодических осмотров);

14) механик (Ф.И.О., фактическое место проживания и контактные телефоны водителей автомобилей);

15) заведующий хозяйством (Ф.И.О место проживания и контактные телефоны работников, находящихся в подчинении);

6.2 Право доступа к персональным данным граждан, признанных нуждающимися в предоставлении социальных услуг имеют:

директор учреждения;

заместители директора по направлению деятельности;

специалисты по социальной работе ОМО, ОСО, ОРИФСО;

ведущий специалист ГО и ЧС (информация о фактическом месте проживания и контактные телефоны получателей социальных услуг, подпадающих в зону подтопления);

программист (системный администратор системы персональных данных);

социальный работник ОСО (информация необходимая для предоставления социальных услуг);

экономист (информация о начислении и оплате за оказанные социальные услуги).

6.3 Право доступа к персональным данным граждан, обратившихся в учреждение за получением социальных услуг:

директор учреждения;

заместители директора по направлению деятельности;

специалист по социальной работе организационно-методическим отделением (далее – ОМО), специалисты по социальной работе ОМО; специалисты по социальной работе ОРИФСО;

программист (системный администратор системы персональных данных);

специалист по социальной работе, выполняющий трудовые функции заведующего отделением ОССО;

социальные работники ОССО;

юрисконсульт ОССО;

экономист.

6.4 Субъекты персональных данных имеют право:

6.4.1 Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные.

6.4.2 Требовать от Оператора уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных.

6.4.3 Получать от Оператора:

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.

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

6.4.5 Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Оператора при обработке и защите его персональных данных.

6.5 Копировать и делать выписки персональных данных Оператора разрешается исключительно в служебных целях по письменному запросу с разрешения директора Учреждения.

6.6 Передача информации третьей стороне возможна только при письменном согласии субъекта персональных данных.

7. Защита персональных данных и порядок действий в случае запросов надзорных органов

7.1 Защиту персональных данных субъектов от неправомерного их использования или утраты Учреждение обеспечивает за счет собственных средств в порядке, установленном законодательством РФ.

При обработке персональных данных должны быть приняты необходимые организационные и технические меры по обеспечению их конфиденциальности.

Технические меры защиты персональных данных при их обработке техническими средствами устанавливаются в соответствии с установленными действующим законодательством РФ и внутренними документами Учреждения мерами в сфере информационной безопасности обработки персональных данных.

7.2 Защита персональных данных предусматривает ограничение к ним доступа.

7.3 Руководитель структурного подразделения Учреждения, осуществляющего обработку персональных данных:

1) несет ответственность за организацию защиты персональных данных в подчиненном структурном подразделении;

2) закрепляет за работниками, уполномоченными обрабатывать персональные данные, конкретные материальные носители, на которых допускается хранение персональных данных в случае, если такие носители необходимы для выполнения возложенных на работников функций;

3) организывает изучение подчиненными работниками, в чьи обязанности входит обработка персональных данных, нормативных правовых актов по защите персональных данных и требует их неукоснительного исполнения;

4) обеспечивает режим конфиденциальности в отношении персональных данных, обрабатываемых в структурном подразделении;

5) организывает контроль доступа к персональным данным в соответствии с функциональными обязанностями работников подразделения. 7.4 Работники, допущенные к персональным данным, дают письменное обязательство о неразглашении таких данных в установленном порядке.

7.5 В соответствии с частью 4 статьи 20 Федерального закона № 152-ФЗ Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

7.6 Сбор сведений, для составления мотивированного ответа на запрос надзорных органов, осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением работников Учреждения.

7.7 В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

8. Обязанности и ответственность за нарушение норм законодательства в области персональных данных лиц к обработке персональных данных

8.1 Лица, допущенные к работе с персональными данными, обязаны:

1) знать законодательство РФ в области обработки и защиты персональных данных, нормативные документы Учреждения по защите персональных данных;

2) сохранять конфиденциальность персональных данных;

3) обеспечивать сохранность закрепленных за ними носителей персональных данных;

4) контролировать срок истечения действия согласий на обработку персональных данных и при необходимости дальнейшей обработки персональных данных, обеспечивать своевременное получение новых согласий или прекращение обработки персональных данных;

5) докладывать своему непосредственному руководителю отдела (структурного подразделения) обо всех фактах и попытках несанкционированного доступа к персональным данным и других нарушениях.

8.2 В соответствии частью 4 статьи 20 Федерального закона № 152-ФЗ Учреждение сообщает в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение тридцати дней с даты получения такого запроса.

8.3 Сбор сведений для составления мотивированного ответа на запрос надзорных органов осуществляет ответственный за организацию обработки персональных данных при необходимости с привлечением работников Учреждения.

8.4 В течение установленного законодательством срока ответственный за организацию обработки персональных данных подготавливает и направляет в уполномоченный орган мотивированный ответ и другие необходимые документы.

8.5 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ. «О персональных данных».

8.6 Директор Учреждения за нарушение норм, регулирующих получение, обработку и защиты персональных данных субъекта персональных данных, несет административную ответственность согласно статьям 5.27 и 5.39 КоАП РФ, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом субъекте».

Директор



О.А. Басович