

Положение об обработке и защите персональных данных в ФКУ «ГБ МСЭ по Республике Марий Эл» Минтруда России

1. Общие положения

1.1 Настоящее Положение об обработке и защите персональных данных (далее – Положение) в ФКУ «ГБ МСЭ по Республике Марий Эл» Минтруда России (далее – Учреждения) разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации» №149 от 27.07.2006г., Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Правилами внутреннего трудового распорядка Учреждения.

1.2 Цель разработки Положения – определение порядка обработки персональных данных сотрудников Учреждения и иных субъектов персональных данных, персональные данные которых подлежат обработке; обеспечение защиты прав и свобод человека и гражданина, в т.ч. работника Учреждения, при обработке его персональных данных, в том числе защиты прав 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.

1.3 Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено законом.

2. Основные понятия и состав персональных данных

2.1 Для целей настоящего Положения используются следующие основные понятия:

- **под персональными данными субъектов (ПДн)** понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, пол, год, месяц, дата и место рождения, адрес места жительства, контактные телефоны, реквизиты полиса, индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), паспортные данные, данные о состоянии здоровья, заболеваниях;

- **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;

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

- **распространение персональных данных** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- **использование персональных данных** - действия (операции) с персональными данными, совершаемые должностным лицом Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

- **блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

- **уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

- **обезличивание персональных данных** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

- **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

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

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

2.2 Состав персональных данных, обрабатываемых в информационной системе персональных данных (далее – ИСПДн) Учреждения, определяется «Перечнем персональных данных, подлежащих защите» (Приложение №2).

2.3 Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в Учреждении при его приеме, переводе и увольнении.

1) Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника).

2) При оформлении работника в Учреждение, главным специалистом заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

– общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, пол, знание иностранного языка, образование, специальность и квалификация по диплому, профессия, стаж работы, состояние в браке, состав семьи, паспортные данные, адреса мест жительства по паспорту и по факту, номер телефона);

– сведения о воинском учете;

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;

– сведения об аттестации;

– сведения о повышении квалификации;

– сведения о профессиональной переподготовке;

– сведения о наградах (поощрениях), почетных званиях;

– сведения об отпусках;

– сведения о социальных гарантиях;

– дополнительные сведения;

– сведения об увольнении.

3) В отделе кадрово-правового обеспечения создаются и хранятся следующие группы документов, содержащие персональные данные работников в единичном или сводном виде:

– документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу, об отпусках; личные дела, карточки и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; тарификационные списки сотрудников);

– организационно-распорядительная документация Учреждения (Положения, должностные инструкции работников, приказы руководителя); документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

4) В планово-финансовом отделе создаются и хранятся следующие группы документов, содержащих персональные данные работников:

– комплексы документов, содержащих сведения о заработной плате, доплатах и надбавках;

– комплексы документов, содержащих основания для предоставления дополнительных социальных гарантий;

– копии отчетов, направляемых в налоговую инспекцию, территориальные органы Пенсионного фонда, Фонда социального страхования, государственные органы статистики, вышестоящие органы управления и другие учреждения.

5) В отделе по общим вопросам деятельности учреждения хранятся следующие группы документов, содержащие персональные данные:

– дела, содержащие материалы аттестации работников;

– журналы и документы о несчастных случаях;

– журнал учета выдачи изготовленных печатей и штампов, оттиски печатей.

6) В экспертных составах и филиалов-бюро хранятся следующие группы документов, содержащих персональные данные:

– документы и сведения об инвалидности, состоянии здоровья, трудоспособности лиц, прошедших освидетельствование в Учреждении.

2.4 Комплекс документов, сопровождающий процесс проведения медико-социальной экспертизы лиц, нуждающихся в этом.

2.4.1 Информация, представляемая обратившимися в Учреждение гражданами, должна иметь документальную форму. Граждане предъявляют следующие документы:

– паспорт или иной документ, удостоверяющий личность;

– направление на медико-социальную экспертизу;

– личное заявление;

– иные документы необходимые для проведения медико-социальной экспертизы.

В дальнейшем в Учреждении обрабатываются персональные данные, указанные в Перечне персональных данных, подлежащих защите.

3. Сбор, обработка и защита персональных данных

3.1 Порядок получения персональных данных.

3.1.1 Все персональные данные сотрудников Учреждения и прочих физических лиц следует получать у них самих. Если персональные данные возможно получить только у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Учреждения должно сообщить о целях, предполагаемых источниках и способах получения персональных данных, а

также о характере подлежащих получению персональных данных и последствиях отказа субъекта дать письменное согласие на их получение.

3.1.2 Учреждение не имеет права получать и обрабатывать персональные данные сотрудников об их расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни.

3.1.3 Учреждение как работодатель вправе обрабатывать персональные данные сотрудников и прочих физических лиц только с их письменного согласия.

3.1.4 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 определяющего полномочия работодателя;

- обработка персональных данных осуществляется в целях исполнения 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 работника, если получение его согласия невозможно.

3.2 Порядок обработки, передачи и хранения персональных данных.

3.2.1 Субъект предоставляет должностному лицу Учреждения достоверные сведения о себе. Должностное лицо проверяет достоверность сведений, сверяя данные, предоставленные субъектом, с имеющимися у субъекта документами.

3.2.2 Руководитель и сотрудники Учреждения (операторы) при обработке персональных данных должны соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов проведения медико-социальной экспертизы лиц, нуждающихся в этом, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

- при определении объема и содержания обрабатываемых персональных данных сотрудник должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ и иными федеральными законами.

- при принятии решений, затрагивающих интересы субъекта, Учреждение, как оператор, не имеет права основываться на персональных данных субъекта, полученных исключительно в результате их автоматизированной обработки или электронного получения.

- защита персональных данных субъекта от неправомерного их использования или утраты обеспечивается Учреждением как оператором за счет своих средств в порядке, установленном федеральным законом.
- сотрудники и их представители должны быть ознакомлены под подпись с документами Учреждения, устанавливающими порядок обработки персональных данных, а также об их правах и обязанностях в этой области.
- во всех случаях отказ субъекта от своих прав на сохранение и защиту персональных данных недействителен.

4. Передача и хранение персональных данных

4.1 При передаче персональных данных субъекта Учреждение должно соблюдать 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, а также в случаях, установленных федеральным законом.

2) 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 подтверждения того, что это правило соблюдено. Лица, получившие персональные данные субъекта, обязаны соблюдать режим конфиденциальности. Данное Положение не распространяется на обмен персональными данными субъектов в порядке, установленном федеральными законами.

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

4) 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.

5) Передавать персональные данные представителям в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными субъекта, которые необходимы для выполнения указанными представителями их функции.

4.2 Хранение и использование персональных данных.

4.2.1 Персональные данные субъектов обрабатываются и хранятся в помещениях Учреждения и на машинных носителях.

4.2.2 Персональные данные субъектов могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде – в локальной компьютерной сети, в компьютерных программах и электронных базах данных.

4.3 При получении персональных данных не от субъекта (за исключением случаев, если персональные данные были предоставлены Учреждению на основании федерального закона или если персональные данные являются общедоступными), Учреждение до начала обработки таких персональных данных обязано предоставить субъекту следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом №152 «О персональных данных» права субъекта персональных данных.

5. Доступ к персональным данным

5.1 Перечень лиц, имеющих право доступа к персональным данным, определяется «Перечнем лиц, осуществляющих обработку персональных данных, либо имеющих к ним доступ» (Приложение №3), утвержденным Руководителем Учреждения.

5.2 Субъект персональных данных, чьи персональные данные обрабатываются в информационной системе Учреждения имеет право:

1) Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные этого субъекта.

2) Требовать от Учреждения уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для оператора персональных данных.

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.

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

5) Копировать и делать выписки персональных данных субъекта разрешается исключительно в служебных целях с письменного разрешения руководителя Учреждения.

5.3 Передача информации третьей стороне возможна только при письменном согласии субъектов.

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

6.1 Работники Учреждения, виновные в нарушении норм, регулирующих получение, хранение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.

6.2 Ответственность за утрату документов или машиночитаемых носителей с конфиденциальной информацией или разглашение сведений, содержащихся в них, персонально несет работник, допустивший их утрату (разглашение).

6.3 Разглашение конфиденциальной информации или утрата документов, машиночитаемых носителей информации, содержащих персональные данные и иную конфиденциальную информацию, влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, а также договорными обязательствами между работодателем и принятым на работу работником, закрепленным трудовым договором.

6.4 По факту разглашения сведений или утраты документов распоряжением руководителя Учреждения назначается комиссия для проведения служебного расследования.

6.5 Комиссия, проводившая служебное расследование, принимает меры по локализации нежелательных последствий разглашения конфиденциальной информации, устанавливает обстоятельства происшествия и виновных в утрате (разглашении), а также причины и условия, способствующие этому.

6.6 Служебное расследование проводится в 2-недельный срок со дня обнаружения факта разглашения (утраты). По результатам расследования руководителем Учреждения принимается решение о привлечении виновных лиц к ответственности, предусмотренной законодательством Российской Федерации.

6.7 Законодательством Российской Федерации за нарушение правил защиты информационных ресурсов при их использовании предусмотрена уголовная, административная и дисциплинарная ответственность.

Перечень персональных данных, подлежащих защите в ФКУ «ГБ МСЭ по Республике Марий Эл» Минтруда России

1. Общие положения

Объектами защиты являются – информация, обрабатываемая в ФКУ «ГБ МСЭ по Республике Марий Эл» Минтруда России и технические средства ее обработки и защиты.

Объекты защиты включают:

- 1) Обрабатываемая информация: персональные данные субъектов ПДн и персональные данные сотрудников
- 2) Технологическая информация.
- 3) Программно-технические средства обработки.
- 4) Средства защиты ПДн.
- 5) Каналы информационного обмена и телекоммуникации.
- 6) Объекты и помещения, в которых размещены компоненты ИСПДн.

2. Обрабатываемая информация

2.1 Перечень персональных данных субъектов ПДн

Персональные данные субъектов ПДн (пациентов) включают:

- ФИО;
- Пол;
- Дата рождения;
- Контактный телефон;
- Адрес прописки;
- Адрес фактического проживания;
- Паспортные данные (данные документа, удостоверяющего личность гражданина РФ);
- СНИЛС (страховой номер индивидуального лицевого счета гражданина в системе персонифицированного учета Пенсионного фонда России);
- Информация об образовании (наименование и адрес образовательного учреждения, группа, класс, курс);
- Информация о трудовом стаже и деятельности (должность, профессия, специальность, квалификация и стаж работы на указанной должности на момент направления на медико-социальную экспертизу; основная профессия, квалификация по основной профессии);
- Данные о состоянии здоровья (история болезни, анамнез жизни).

2.2 Перечень персональных данных сотрудников Учреждения

Персональные данные сотрудников Учреждения включают:

- Фамилия, имя, отчество;
- Место, год и дата рождения;
- Адрес по прописке и адрес проживания;

- Паспортные данные (серия, номер паспорта, кем и когда выдан);
- Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
- Информация о трудовой деятельности до приема на работу (место предыдущей работы, должность, период работы, причины увольнения);
 - Телефонный номер (домашний, рабочий, мобильный);
 - Семейное положение и состав семьи (муж/жена, дети);
 - Пол;
 - Информация о знании иностранных языков;
 - Форма допуска;
 - Оклад;
- Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
- Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
 - ИНН;
 - Данные о переводах на другую работу;
 - Данные об аттестации работников;
 - Данные о повышении квалификации;
 - Данные о профессиональной переподготовке;
 - Данные о наградах, медалях, поощрениях, почетных званиях;
 - Информация о приеме на работу, перемещении по должности, увольнении;
 - Информация об отпусках;
 - Информация о командировках;
 - Информация о болезнях;
 - Информация о социальных гарантиях;
 - Информация о негосударственном пенсионном обеспечении.

2.3 Технологическая информация

- Технологическая информация, подлежащая защите, включает:
- управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
 - технологическая информация средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
 - информация на съемных носителях информации (бумажные,

магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;

- информация о СЗПДн, их составе и структуре, принципах и технических решениях защиты;

- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;

- служебные данные (метаданные) появляющиеся при работе программного обеспечения, сообщений и протоколов межсетевого взаимодействия, в результате обработки Обрабатываемой информации.

2.4 Программно-технические средства обработки

Программно-технические средства включают в себя:

- общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);

- резервные копии общесистемного программного обеспечения;

- инструментальные средства и утилиты систем управления ресурсами ИСПДн;

- аппаратные средства обработки ПДн (АРМ и сервера);

- сетевое оборудование (коммутаторы, маршрутизаторы и т.п.).

2.5 Средства защиты ПДн

Средства защиты ПДн состоят из аппаратно-программных средств, включают в себя:

- средства управления и разграничения доступа пользователей;

- средства обеспечения регистрации и учета действий с информацией;

- средства, обеспечивающие целостность данных;

- средства антивирусной защиты;

- средства межсетевого экранирования;

- средства анализа защищенности;

- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

2.6 Каналы информационного обмена и телекоммуникации

Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

2.7 Объекты и помещения, в которых размещены компоненты ИСПДн

Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.