

Согласовано  
Председатель профкома ГКУЗ АО  
«Специализированный дом ребенка  
«Капелька»

Утверждаю  
Главный врач ГКУЗ АО  
«Специализированный дом ребенка  
«Капелька»

 /О.В. Григорьев  
 /О.А. Иноземцева/  
« 23 » июля 2013 г. « 23 » июля 2013 г.

**ПОЛОЖЕНИЕ**  
о защите персональных данных работников  
государственного казенного учреждения здравоохранения  
Астраханской области «Специализированный дом ребенка «Капелька»  
(ГКУЗ АО «СДР «Капелька»)

**1. Общие положения**

- 1.1. Целью данного Положения является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.
- 1.2. Настоящее Положение разработано на основании статей Трудового Кодекса РФ, Федерального закона от 27.06.2006 г. №152-ФЗ «О персональных данных».
- 1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях их обезличивания.
- 1.4. Настоящее Положение утверждается и вводится в действие приказом главного врача и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

**2. Понятие и состав персональных данных**

- 2.1. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.
- 2.2. В состав персональных данных работника входят:
  - фамилия, имя, отчество;
  - дата и место рождения;
  - биографические данные;
  - паспортные данные;
  - информация, содержащаяся в трудовой книжке;

- информация, содержащаяся в страховом свидетельстве государственного пенсионного страхования;
  - индивидуальный налоговый номер;
  - информация, содержащаяся в страховом медицинском полисе;
  - сведения об образовании;
  - сведения о трудовом стаже;
  - сведения о составе семьи;
  - сведения о воинском учете;
  - сведения о заработной плате;
  - сведения о международной дебетовой (зарплатной) карте;
  - сведения о социальных льготах;
  - специальность;
  - занимаемая должность;
  - наличие судимостей;
  - адрес места жительства;
  - домашний телефон;
  - место работы или учебы членов семьи и родственников;
  - содержание трудового договора;
  - подлинники и копии приказов по личному составу;
  - личное дело;
  - основания к приказам по личному составу;
  - материалы по повышению квалификации, профессиональной переподготовке, аттестации, служебным расследованиям;
  - копии отчетов, направляемые в вышестоящие организации и в органы статистики.
- 2.3. Данные документы являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

### **3. Обработка персональных данных**

3.1. Под обработкой персональных данных подразумеваются:

- сбор;
- систематизация;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- использование — «действия (операции) с персональными данными, совершаемые в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работника, либо иным образом затрагивающих права и свободы работника;
- распространение (в том числе передача) — «действия, направленные на передачу персональных данных определенному кругу лиц;

- обезличивание — «действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных»;
  - блокирование — «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».
- 3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:
- 3.2.1. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества и для др. случаев, предусмотренных законодательством РФ.
  - 3.2.2. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами РФ.
  - 3.2.3. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.
  - 3.2.4. Персональные данные следует получать от самого работника. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
  - 3.2.5. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.
  - 3.2.6. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.
- 3.3. Перечень лиц, имеющих доступ к обработке, передаче и хранению персональных данных работника утверждается приказом главного врача.
- 3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

- 3.4.1. 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.
- 3.5. Передача персональных данных работника возможна только с письменного согласия работника или в случаях, прямо предусмотренных законодательством.
- 3.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:
- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
  - не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
  - предупредить лиц, получающих персональные данные работника, 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 работника, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами, Трудовым кодексом РФ;
  - разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
  - не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
  - передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.
- 3.5.2. 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.
- 3.5.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.
- 3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

- 3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
- 3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.
- 3.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.
- 3.10. Способы обработки персональных данных.

Обработка персональных данных может осуществляться двумя способами:

- 3.10.1. с использованием средств автоматизации, включающая в себя обработку информации с применением программных продуктов. В ГКУЗ АО «СДР «Капелька»- это:

- система бухгалтерского учета
- картотека сотрудников – центральное место хранения информации о работниках учреждения. Все необходимые сведения о том или ином сотруднике сгруппированы в его Личной карточке. Личная карточка содержит более 20 информационных разделов, где отражаются общие, профессиональные, военно-учетные и прочие данные, условия найма, накопленный стаж, а также отслеживается «история» работы сотрудника на предприятии (движения по службе, взыскания, поощрения и т.д.). Кроме того, реквизитный состав личной карточки может быть расширен по усмотрению пользователя. Личные карточки формируются только на основании приказов о приеме на работу. На основании данных, представленных в личной карточке, обеспечивается полное заполнение форм Т-2 «Личная карточка работника»

- 3.10.2. Обработка персональных данных без использования средств автоматизации – это обработка информации вручную (информация на бумажных носителях, а также обработка информации с использованием компьютерной техники).

#### **4. Доступ к персональным данным**

- 4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Право доступа к персональным данным сотрудника имеют лица, указанные в пункте 3.3. настоящего Положения, а также сам работник - носитель данных.

- 4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести следующие функциональные структуры:

- вышестоящие организации (министерства и ведомства);
- налоговые органы;
- правоохранительные органы;
- органы статистики;
- медицинские страховые фирмы;
- отделы военного комиссариата (для лиц, подлежащих воинскому учету);
- органы социального страхования;

- пенсионные фонды;
  - медицинские учреждения г. Астрахани и Астраханской области с целью проведения обязательных медицинских осмотров, диспансеризации, предварительных и периодических медицинских осмотров;
- 4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.
- 4.2.3. Организации, в которые сотрудник 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.
- 4.2.4. Другие организации и частные лица:
- сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии заявления работника, заверенного в установленном порядке.
  - персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

## **5. Защита персональных данных**

- 5.1. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивающий достаточно надежную безопасность информации в процессе деятельности учреждения.
- 5.2. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.
- 5.3. Внутренняя защита
- 5.3.1. Для обеспечения внутренней защиты персональных данных работников 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;
  - знание работником требований нормативно – методических документов по защите информации и сохранении тайны;
  - наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
  - организация порядка уничтожения информации;
  - своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
  - воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только главному врачу, работникам отдела кадров и в исключительных случаях, по письменному разрешению главного врача, - руководителю структурного подразделения (например, при подготовке материалов для аттестации работника).
- необходимо знать требования инструкций касающихся защиты персональных данных при обработке персональных данных с использованием средств вычислительной техники.

5.3.2. Для защиты персональных данных сотрудника на вычислительной технике и электронных носителях необходимо:

- знание работником инструкции пользователя вычислительной техники;
- разграничение доступа к персональным данным хранящимся на вычислительной технике (имена пользователей и пароли сообщаются соответствующим работникам а также программисту);
- использование средств антивирусной защиты;
- знание работником мер по предотвращению вирусного заражения;
- использование межсетевое экрана;
- использование лицензионного программного обеспечения.

5.4. Внешняя защита:

5.4.1. 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.

5.4.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения, 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 кадров.

5.4.3. Для обеспечения внешней защиты персональных данных сотрудников соблюдаются следующие меры:

- пропускной режим организации;
- технические средства охраны, сигнализации;
- охрана территории и здания.

5.5. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5.6. По возможности персональные данные обезличиваются.

## **6. Права и обязанности работника**

- 6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.
- 6.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.
- 6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:
- на подтверждение факта обработки персональных данных оператором, а также цель такой обработки;
  - узнавать способы обработки персональных данных, применяемые в учреждении;
  - на сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
  - узнавать перечень обрабатываемых персональных данных и источник их получения;
  - узнавать сроки обработки персональных данных, в том числе сроки их хранения;
  - на сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных;
  - требовать исключения или исправления неверных или неполных персональных данных;
  - на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
  - определять своих представителей для защиты своих персональных данных;
  - на сохранение и защиту своей личной и семейной тайны.
- 6.4. Работник обязан:
- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ;
  - своевременно сообщать работодателю об изменении своих персональных данных;
- 6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, должности, специальности, присвоении квалификационной категории и пр.

## **7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными**

- 7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
- 7.2. Юридическое лицо, в соответствии со своими полномочиями владеющее информацией о гражданах, получающее и использующее ее, несет ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.



- 7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
- 7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.
- 7.5. 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.
- 7.5.1. 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.
- 7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, 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.
- 7.5.3. 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.
- 7.5.4. 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.
- 7.6. Работодатель обязан сообщить субъекту персональных данных или его законному представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с ними при обращении субъекта персональных данных или его законного представителя либо в течение десяти рабочих дней с даты получения запроса субъекта персональных данных или его законного представителя.

- 7.7. Работодатель обязан безвозмездно предоставить субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных, а также внести в них необходимые изменения, уничтожить или заблокировать соответствующие персональные данные по предоставлению субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки. О внесенных изменениях и принятых мерах оператор обязан уведомить субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы.
- 7.9. Работодатель обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа, в течение семи рабочих дней с даты получения такого запроса.
- 7.10. В случае выявления недостоверных персональных данных или неправомерных действий с ними при обращении или по запросу субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных работодатель обязан осуществить блокирование персональных данных, относящихся к соответствующему субъекту персональных данных, с момента такого обращения или получения такого запроса на период проверки.
- 7.11. В случае подтверждения факта недостоверности персональных данных оператор на основании документов, представленных субъектом персональных данных или его законным представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные и снять их блокирование.
- 7.12. В случае выявления неправомерных действий с персональными данными оператор в срок, не превышающий трех рабочих дней с даты такого выявления, обязан устранить допущенные нарушения. В случае невозможности устранения допущенных нарушений оператор в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, обязан уничтожить персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.
- 7.13. В случае достижения цели обработки персональных данных оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено федеральными законами, и уведомить об этом субъекта

персональных данных или его законного представителя, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

- 7.14. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.