

ПОЛОЖЕНИЕ

26.11.2015



Директор МБУК г.о. Самара «СМИБС»

Гаврилина Т.В.

О порядке обработки и защиты персональных данных работников МБУК г.о. Самара «СМИБС»

Введено в действие приказом  
От 26 ноября 2015г. № 171

## 1. Общие положения

1.1. Настоящее Положение разработано в целях обработки и защиты персональных данных работников муниципального бюджетного учреждения культуры городского округа Самара «Самарская муниципальная информационно-библиотечная система» (далее по тексту – Учреждение) от несанкционированного доступа.

1.2. Настоящее Положение разработано в соответствии с требованиями Конституции РФ, Трудового кодекса РФ, Кодекса РФ об административных правонарушениях, Гражданского кодекса РФ, Уголовного кодекса РФ, Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" и определяет особенности обработки персональных данных работника.

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

1.4. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.5. Настоящее Положение утверждается директором Учреждения и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным работников.

## 2. Основные понятия

В настоящем Положении используются следующие основные понятия:

2.1 **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.2 **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;

2.3 **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;

2.4 **распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

2.5 **автоматизированная обработка персональных данных** - обработка

персональных данных с помощью средств вычислительной техники;

2.6 **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

2.7 **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

2.8 **блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

2.9 **уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

2.10 **обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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

2.12 **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;

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

2.14 **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.

### 3. Состав персональных данных

3.1. В соответствии с ТК РФ, локальными нормативными актами Учреждения, лицо, поступающее на работу, предъявляет работодателю следующие документы, содержащие его персональные данные:

- паспорт, сведения о месте регистрации (месте жительства), сведения о семейном положении;
- трудовую книжку, содержащую данные о трудовой деятельности работника;
- страховое свидетельство государственного пенсионного страхования, содержащее сведения о номере и серии страхового свидетельства;
- свидетельство о постановке на учет в налоговом органе, содержащее сведения об идентификационном номере налогоплательщика;
- документы воинского учета, содержащие сведения о воинском учете военнообязанных и лиц, подлежащих призыву на военную службу;
- документ об образовании, о квалификации или о наличии специальных знаний или специальной подготовки, содержащий сведения об образовании, профессии.

В отдельных случаях с учетом специфики работы в соответствии с Трудовым Кодексом Российской Федерации, иными федеральными законами, указами Президента Российской Федерации и постановлениями Правительства Российской Федерации может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

Запрещается запрашивать другие документы при заключении трудового договора, если иное не предусмотрено законодательством РФ.

3.2. 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.

3.3. Состав персональных данных работника:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате работника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес места жительства, номер домашнего телефона;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки работников;
- дела, содержащие материалы по повышению квалификации и переподготовке работников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

3.4. Данные документы являются конфиденциальными, учитывая их массовость и единое место обработки и хранения, соответствующий гриф ограничения на них не ставится.

#### **4. Обработка персональных данных работников**

4.1. Под обработкой персональных данных работника понимается получение, хранение, передача или любое другое использование персональных данных работника.

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

- 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 и обеспечения сохранности имущества;

- при определении объема и содержания, обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, ТК РФ и иными федеральными законами;

- персональные данные следует получать у него самого. 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;

- 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, в соответствии со ст. 24 Конституции РФ работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;

- работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом;

- 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.

4.3. Перечень лиц, ответственных за организацию обработки персональных данных работника, определяется приказом директора Учреждения.

4.4. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

4.4.1. 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, также, если обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных и в других случаях, установленных законодательством РФ;

- не допускать обработку персональных данных, несовместимых с целями сбора персональных данных;

- не допускать объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;

- предупреждать лица, получающие 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 секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным работников только специально уполномоченным лицам, 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 ТК РФ, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.4.2. 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.

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

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

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

## **5. Права и обязанности работника**

### **5.1. Работник обязан:**

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен ТК РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.

### **5.2. Работник имеет право:**

- получения полной информации о его персональных данных их обработке и защиты (в том числе автоматизированной);
- требовать уточнения, исправления, блокирования или уничтожения устаревших, неточных, неполных или не являющихся необходимыми для заявленной цели обработки персональных данных, а также данных, обработанных с нарушением требований законодательства РФ и настоящего Положения;
- заявить в письменной форме о своем несогласии (с соответствующим обоснованием такого несогласия) в случае отказа работодателя исключить или исправить персональные данные работника;
- дополнить заявлением, выражающим его собственную точку зрения, персональные данные оценочного характера;
- требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- свободного бесплатного доступа к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральным законом;
- определять своих представителей для защиты своих персональных данных;
- обжаловать в суд любые неправомерные действия или бездействие представителя нанимателя или уполномоченного им лица при обработке и защите персональных данных работника.

### **5.3. Работник не должен отказываться от своих прав на сохранение и защиту тайны.**

## **6. Доступ к персональным данным работника**

### **6.1. Внутренний доступ (доступ внутри организации).**

#### **6.1.1. Право доступа к персональным данным работника имеют:**

- директор Учреждения;
- руководители структурных подразделений по направлению деятельности (доступ к личным данным только работников своего подразделения);
- при переводе из одного структурного подразделения в другое, доступ к персональным данным работника может иметь:
  - руководитель нового подразделения;
  - работники отдела кадров;
  - работники отдела экономики и бухгалтерского учета;
  - работники отдела автоматизации;
  - сам работник, носитель данных.

#### **6.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора Учреждения.**

### **6.2. Внешний доступ.**

#### **6.2.1. К числу массовых потребителей персональных данных вне Учреждения можно отнести государственные и негосударственные функциональные структуры:**

- налоговые инспекции;
- правоохранительные органы;
- страховые агентства;
- военкоматы;
- органы социального страхования;

- пенсионные фонды.

6.2.2. Государственные и муниципальные органы контроля имеют доступ к информации только в сфере своей компетенции.

6.2.3. 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.

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

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

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

## 7. Защита персональных данных

7.1. 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.

7.2. 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.

7.3. Защита персональных данных представляет собой жестко регламентированный и динамически развивающийся 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 Учреждения.

7.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет собственных средств в порядке, установленном федеральным законом.

7.5. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами Учреждения.

7.6. Внутренняя защита:

7.6.1. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников Учреждения, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при которых исключалось бы бесконтрольное использование защищаемой информации;
- 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;
- определение состава работников, имеющих право доступа (входа) в помещение, в

котором находится сервер;

- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа работниками Учреждения;
- воспитательная и разъяснительная работа с работниками Учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел работников на рабочие места.

#### 7.6.2. Защита персональных данных работника на электронных носителях.

Все папки, содержащие персональные данные работника, должны быть защищены паролем, который сообщается начальнику отдела правовой и кадровой работы и заведующему отделом автоматизации и информационных технологий Учреждения.

#### 7.7. Внешняя защита:

7.7.1. 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.

7.7.2. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе правовой и кадровой работы.

7.7.3. Для обеспечения внешней защиты персональных данных работников применяются технические средства охраны;

7.8. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны ознакомиться под роспись с настоящим Положением и подписать Соглашение о неразглашении персональных данных работников (Приложение № 1).

7.9. По возможности персональные данные обезличиваются.

7.10. По истечении срока хранения, персональные данные работников уничтожаются.

7.11. Работники и их представители должны быть ознакомлены под роспись с документами Учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

### **8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника**

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

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

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

8.4. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут в соответствии с федеральными законами ответственность:

- дисциплинарную (замечание, выговор, увольнение);
- административную (предупреждение или административный штраф);
- гражданско-правовую (возмещение причиненного ущерба).

8.5. Работник, предоставивший работодателю подложные документы или заведомо ложные сведения о себе, несет дисциплинарную ответственность, вплоть до увольнения.

8.6. Повседневный контроль за соблюдением данного Положения возлагается на начальника отдела кадров.

8.7. Периодический контроль за соблюдением данного Положения возлагается на

заместителей директора с соответствующими обязанностями.

## **9. Заключительные положения**

9.1. Настоящее Положение вступает в силу с момента его утверждения директором и вводится в действие приказом директора Учреждения.

Положение обязательно для всех работников Учреждения, если иные условия не предусмотрены в трудовом договоре работника.

Директор Учреждения вправе вносить изменения и дополнения в настоящее Положение. Работники Учреждения должны быть поставлены в известность о вносимых изменениях и дополнениях за 5 дней до вступления их в силу посредством издания директором приказа и ознакомления с ним всех работников Учреждения.



