

«УТВЕРЖДАЮ»

Директор ГБУК «СОИКМ им. П. В. Алабина»

В.Н. Лисейчев

2017г.



ПОЛОЖЕНИЕ

о порядке организации обработки и
обеспечении безопасности персональных данных в

**государственном бюджетном учреждении культуры
«Самарский областной историко-краеведческий музей им. П.В.
Алабина»**

г. Самара

1. Общие положения

1.1. Настоящее Положение обработке персональных данных работников (далее — Положение) государственного бюджетного учреждения культуры «Самарский областной историко-краеведческий музей им. П.В. Алабина» (далее – Учреждение) разработано в соответствии с Трудовым кодексом Российской Федерации (Федеральным законом от 30.12.2001 № 197-ФЗ), Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»; Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781; Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687., Законом РФ от 09.10.1992 № 3612-1 «Основы законодательства Российской Федерации о культуре»; Устава, утвержденного Приказом № 492-р министра культуры Самарской области от 22.07.2011г.; Правилами внутреннего трудового распорядка Учреждения.

1.2. Цель разработки Положения — определение порядка обработки персональных данных работников Учреждения; обеспечение защиты прав и свобод работников Учреждения при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников Учреждения, за невыполнение требований норм, регулирующих обработку и защиту персональных данных. В отношении сведений о физических лицах, позволяющих идентифицировать его личность, за исключением обезличенных и общедоступных персональных данных, в установленных федеральными законами случаях, должна обеспечиваться конфиденциальность таких сведений.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения директором Учреждения и действует бессрочно, до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом директора.

1.4. Все работники Учреждения должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения.

2. Основные понятия и состав персональных данных работников

2.1. Для целей настоящего Положения используются следующие основные понятия^[1]:

- персональные данные работника — любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;
- обработка персональных данных — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных работников Учреждения;
- конфиденциальность персональных данных — обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным работников, требование не допускать их распространения без согласия работника или иного законного основания;
- распространение персональных данных — действия, направленные на передачу персональных данных работников определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников 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 работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных работников, в том числе их передачи;
- уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных работников или в результате которых уничтожаются материальные носители персональных данных работников;
- обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику;
- общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия работника 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 информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

2.2. В состав персональных данных работников Учреждения входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы.

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

2.3.1. Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. Объем документов, предъявляемых работником определен ст. 65 ТК РФ.

2.3.2. При оформлении работника в Учреждение работником отдела кадров 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, образование, профессия, стаж работы, состояние в браке, паспортные данные);

– сведения о воинском учете;

– данные о приеме на работу;

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;

– сведения о месте жительства и контактных телефонах.

2.3.3. В отделе кадров Организации создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.3.3.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по

личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных 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).

2.3.3.2. Документация по организации работы структурных подразделений (положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства Учреждения); документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

3. Сбор, обработка и защита персональных данных

3.1. Порядок получения персональных данных.

3.1.1. Все персональные данные работника Учреждения 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. Должностное лицо работодателя должно сообщить работнику Организации 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^[4].

3.1.2. Работодатель не имеет права получать и обрабатывать персональные данные работника Учреждения о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия^[5].

Обработка указанных персональных данных работников работодателем возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
- по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом^[6].

3.1.3. Работодатель вправе обрабатывать персональные данные работников только с их письменного согласия.

3.1.3.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона № 152-ФЗ;

- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Самарской области, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона № 152-ФЗ;

- после принятия необходимых мер по защите персональных данных.

3.1.4. Письменное согласие работника 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 выдавшем его органе;

– наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

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

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

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

Форма заявления о согласии работника на обработку персональных данных см. в приложении 1 к настоящему Положению.

3.1.5. Согласие работника не требуется в следующих случаях:

1) 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;

2) обработка персональных данных осуществляется в целях исполнения трудового договора;

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

4) 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. Работник Учреждения предоставляет работнику отдела кадров достоверные сведения о себе. Работник отдела кадров Учреждения проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

3.2.2. В соответствии со ст. 86, гл. 14 ТК РФ в целях обеспечения прав и свобод человека и гражданина директор Учреждения (Работодатель) и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

3.2.2.1. Обработка персональных данных 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;

3.2.2.2. При определении объема и содержания, обрабатываемых персональных данных Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

3.2.2.3. 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.

3.2.2.4. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается Работодателем за счет его средств в порядке, установленном федеральным законом.

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

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

3.3. Обработка персональных данных может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

3.4. ЗАПРЕЩАЕТСЯ:

- обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке;
- осуществлять ввод персональных данных под диктовку.

4. Передача и хранение персональных данных

4.1. При передаче персональных данных работника Работодатель должен соблюдать следующие требования^[13]:

4.1.1. 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.

4.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

4.1.3. Предупредить лиц, получивших 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, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

4.1.4. Осуществлять передачу персональных данных работников в пределах Учреждения в соответствии с настоящим Положением.

4.1.5. 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 конкретной функции.

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

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

4.2. Хранение и использование персональных данных работников.

4.2.1. Персональные данные работников обрабатываются и хранятся в отделе кадров.

4.2.2. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде — локальной компьютерной сети и компьютерной программе «1С: Зарплата и кадры».

4.3. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику 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 настоящим Федеральным законом права субъекта персональных данных.

5. Доступ к персональным данным работников

5.1. Право доступа к персональным данным работников имеют:

- директор Учреждения;
- сотрудники отдела кадров;
- сотрудники бухгалтерии;
- начальник отдела экономической безопасности (информация о фактическом месте проживания и контактные телефоны работников);
- начальник отдела внутреннего контроля (доступ к персональным данным работников в ходе плановых проверок);
- руководители структурных подразделений по направлению деятельности (доступ к персональным данным только работников своего подразделения).

5.2. Работник Учреждения имеет право:

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

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

5.2.3. Получать от Работодателя

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

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

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

5.3. Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения начальника отдела кадров.

5.4. Передача информации третьей стороне возможна только при письменном согласии работников.

6. Обеспечение безопасности обработки персональных данных

6.1. В целях обеспечения безопасности персональных данных при их обработке в Учреждении:

- установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ, в соответствии с пунктом 2.4 настоящего Положения;

- обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- обеспечивать пропускной режим в соответствии с утвержденными документами по охране и осуществлению пропускного режима;

- помещения, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц;

- доступ к информации в электронном виде должен осуществляться с использованием парольной защиты, а в информационных системах персональных данных - с использованием средств автоматизации в соответствии с нормативными документами;

- электронные носители информации, содержащие персональные данные, учитываются в журнале учета электронных носителей персональных данных.

6.2. Обеспечение безопасности персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781, нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

6.3. Мероприятия по обеспечению безопасности персональных данных проводятся в соответствии с Положением о методах и способах защиты информации в информационных системах персональных данных утвержденных приказом ФСТЭК России от 05.02.2010 № 58

6.4. Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых ГБУК СОИКМ им П. В. Алабина угроз безопасности персональных данных (модели угроз) и в зависимости от

класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. N 55/86/20

6.5. Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе системы защиты персональных данных.

6.6. Обеспечение безопасности персональных данных в информационных системах персональных данных без использованием средств автоматизации осуществляется в соответствии с требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.

6.7. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

6.8. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);

6.9. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных должны соблюдаться условия изложенные в п.7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации

6.10. Неавтоматизированная обработка персональных данных в электронном виде осуществляется как правило на внешних электронных носителях информации. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

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

7.1. Работники Учреждения, 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.

7.2. Директор Учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные работника.

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: глава 1, ст. 3.

[2] Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», ст. 2.

[3] В законодательно определенных случаях может предусматриваться необходимость предъявления при заключении трудового договора дополнительных документов.

[4] ТК РФ, гл. 14, ст. 86, п. 3.

[5] ТК РФ, гл. 14, ст. 86, п. 4.

[6] ТК РФ, гл. 14, ст. 86, п. 5.

[7] ТК РФ, гл. 14, ст. 86, п. 1.

[8] ТК РФ, гл. 14, ст. 86, п. 2.

[9] ТК РФ, гл. 14, ст. 86, п. 6.

[10] ТК РФ, гл. 14, ст. 86, п. 7.

[11] ТК РФ, гл. 14, ст. 86, п. 8.

[12] ТК РФ, гл. 14, ст. 86, п. 9.

[13] ТК РФ, гл. 14, ст. 88.

[14] ТК РФ, гл. 14, ст. 87.