



**МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«МУНИЦИПАЛЬНЫЙ АРХИВ ГОРОДА КЕРЧИ»**

П Р И К А З

14 января 2016 года

г. Керчь

№ 8

Об организации работы с персональными данными работников Муниципального казенного учреждения «Муниципальный архив города Керчи»

На основании Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», с целью организации работы по обработке и защите персональных данных в Муниципальном казенном учреждении «Муниципальный архив города Керчи» ПРИКАЗЫВАЮ:

1. Утвердить Положение о работе с персональными данными работников Муниципального казенного учреждения «Муниципальный архив города Керчи» (приложение 1).

2. Утвердить Перечень должностей работников Муниципального казенного учреждения «Муниципальный архив города Керчи», ответственных за организацию обработки персональных данных работников и их защиту (приложение 2).

3. Утвердить Перечень должностей работников Муниципального казенного учреждения «Муниципальный архив города Керчи», имеющих право доступа к персональным данным работников, в том числе в программе «1С: Зарплата и кадры государственного учреждения», при исполнении ими должностных обязанностей, связанных с трудовыми функциями, на которых распространяется ответственность по защите персональных данных при их обработке (приложение 3).

4. Утвердить Перечень должностей работников Муниципального казенного учреждения «Муниципальный архив города Керчи», имеющих право доступа к персональным данным работников, при исполнении ими

должностных обязанностей, связанных с трудовыми функциями, на которых распространяется ответственность по защите персональных данных при их обработке (приложение 4).

5. Утвердить Перечень лиц, ответственных за охрану труда, пожарную безопасность и воинский учет в Муниципальном казенном учреждении «Муниципальный архив города Керчи», имеющих право доступа к персональным данным при выполнении возложенных обязанностей, на которых распространяется ответственность по защите персональных данных при их обработке (приложение 5).

6. Контроль за исполнением приказа оставляю за собой.

Директор муниципального архива

Е.С.Плужникова

Приложение 1
к приказу Муниципального казенного
учреждения «Муниципальный архив
города Керчи»
от 14 января 2016 г. № 8

Положение о работе с персональными данными работников
Муниципального казенного учреждения
«Муниципальный архив города Керчи»

I. Общие положения

1.1. Положение о работе с персональными данными работников Муниципального казенного учреждения «Муниципальный архив города Керчи» (далее - Положение) определяет основные требования к порядку обработки персональных данных работников Муниципального казенного учреждения «Муниципальный архив города Керчи» (далее - работники) в соответствии с законодательством Российской Федерации.

1.2. Положение разработано в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, федеральными законами от 27.07.2006 № 152-ФЗ «О персональных данных», 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и иными федеральными законами с целью защиты прав и свобод работника при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну и является документом, регламентирующим работу каждого работника в части обеспечения безопасности персональных данных в Муниципальном казенном учреждении «Муниципальный архив города Керчи» (далее – архив).

Работодатель осуществляет обработку персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Трудовым кодексом Российской Федерации.

1.3. В Положении используются следующие основные понятия:

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

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.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Общедоступные персональные данные – источники персональных данных (в том числе справочники, адресные книги), созданные в целях информационного обеспечения с письменного согласия субъекта персональных данных. В общедоступные источники персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных. Сведения о субъекте персональных данных исключаются в любое время из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

Конфиденциальность персональных данных – операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Оператор персональных данных работников – работники архива, которые самостоятельно или совместно с другими лицами осуществляют обработку персональных данных, а также определяют цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Пользователь информационной системы персональных данных – специально уполномоченное лицо, допущенное к базе персональных данных информационной системы и имеющее право обрабатывать персональные данные работников в пределах, определенных его конкретными функциями.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях её материальный носитель.

II. Состав информации персонального характера

2.1. Персональные данные работника содержатся в документах персонального учета и других документах, отражающих процедуру документирования трудовых отношений.

2.2. К документам, содержащим информацию персонального характера, относятся следующие документы и их комплексы:

2.2.1. Документы персонального характера, удостоверяющие личность работника или содержащие сведения о работнике (об образовании, состоянии здоровья, трудовом стаже и др.): паспорт работника или иной документ, удостоверяющий личность, военный билет, страховое свидетельство государственного пенсионного страхования, документы об образовании (дипломы, свидетельства, сертификаты, удостоверения и др.), трудовая книжка работника, медицинские справки, заключения и др.

2.2.2. Документы по учету кадров: приказы (постановления, распоряжения) о приеме (заключении трудового договора), переводе, увольнении (прекращении трудового договора), предоставлении отпусков, поощрении, взыскании, личная карточка (ф. № Т-2), личное дело работника, вспомогательные регистрационно - учетные формы (книжки, журналы, картотеки, базы данных), содержащие персональные данные работников: журналы регистрации приказов по личному составу, о предоставлении ежегодных оплачиваемых отпусков, отпусков без сохранения заработной платы, по беременности и родам, по уходу за ребенком до достижения им возраста полутора лет, трех лет, о командировании работников, о дисциплинарных взысканиях, книга учета движения трудовых книжек и вкладышей к ним, журнал учета выдачи копий трудовых книжек, справок о трудовой деятельности, сведений о страховом стаже застрахованных лиц и другие журналы, содержащие персональные данные работников.

2.2.3. Договоры с работниками о полной материальной ответственности.

2.2.4. Документы, отражающие результаты служебных расследований: докладные и объяснительные записки, акты, справки, протоколы и др.

2.2.5. Документы об установлении работнику должностного оклада, надбавок к должностному окладу, компенсационных выплат, премий и т.д. (основания к приказам по личному составу, приказам о начислении и выплате заработной платы, выделении материальной помощи).

2.2.6. Индивидуальные сведения работника, передаваемые в органы ПФР, налоговые органы, органы социального страхования о стаже и зарплате, отчислениях в фонд социального страхования, периодах временной нетрудоспособности и т.д.

2.2.7. Документы бухгалтерского учета, содержащие информацию о расчетах с работниками: лицевые счета по заработной плате, расчетно - платежные ведомости на выдачу заработной платы, расчетные листки.

2.2.8. Если персональные данные работника содержатся в других документах, на них распространяется действие данного Положения.

2.3. В личное дело работника вносятся его персональные данные и иные сведения, связанные с поступлением на работу, осуществлением трудовой деятельности и увольнением, а также необходимые для обеспечения деятельности архива.

2.4. Личное дело работника может состоять из следующих документов:

- направление на предварительный (при приеме на работу) медицинский осмотр (обследование);
- медицинское заключение по результатам предварительного (периодического) медицинского осмотра (обследования);
- собственноручно заполненная и подписанная анкета с фотографией;
- автобиография;
- письменное заявление о приеме на работу;
- экземпляр трудового договора с приложением к нему;
- копия приказа о приеме на работу;
- должностная инструкция работника;
- согласие на обработку персональных данных;
- обязательство о неразглашении персональных данных работников;
- обязательство о соблюдении конфиденциальности информации;
- письменное заявление о переводе на другую должность;
- копия приказа (распоряжения) о переводе на другую должность;
- экземпляры соглашений об изменении определенных сторонами условий трудового договора, дополнительных соглашений, ученического договора на получение образования без отрыва от работы, заключаемых в письменной форме и являющихся неотъемлемой частью трудового договора;
- заявление работника об увольнении;
- копия приказа об увольнении;
- направление на периодический медицинский осмотр;
- дополнение к анкете (личному листку по учету кадров);
- лист ознакомления с личным делом работника;
- документы, нахождение которых в личном деле будет признано целесообразным, например: заявление о согласии на направление на обучение; копия приказа о направлении на обучение; предложение (заявление работника) о совмещении должностей; соглашение о совмещении должностей; копия приказа о совмещении должностей; заявление о предоставлении отпуска по беременности и родам, копия приказа о предоставлении отпуска по беременности и родам; заявление о предоставлении отпуска по уходу за ребенком, копия приказа о предоставлении отпуска по уходу за ребенком; заявление о внесении изменений в учетные данные (изменение фамилии, места жительства, паспортных данных и др.); приказ о внесении изменений в учетные данные (изменение фамилии, места жительства, паспортных данных и др.);
- другие документы, предусмотренные федеральными законами и иными нормативными правовыми актами Российской Федерации.

III. Сбор персональных данных работника и гарантии их защиты

3.1. 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 статьей 24 Конституции Российской Федерации, работодатель вправе получать данные о частной жизни работника только с его письменного согласия.

Не допускается получение и обработка персональных данных работников о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

Письменное согласие 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 оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование структурных подразделений архива или должностей работников архива, осуществляющих обработку персональных данных по поручению оператора;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

3.2. Все персональные данные работника предоставляются самим работником. Если персональные данные работника могут быть получены только у третьей стороны, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. В согласии на обработку персональных данных, предоставляемом работником при приеме на работу, может входить пункт о предоставлении согласия на передачу персональных данных третьей стороне в рамках трудовых отношений, в том числе связанных с финансово-хозяйственной деятельностью работодателя, а также в случаях оформления работником банковского кредита, виз и других документов, требующих предоставления справок с места работы, по его письменному заявлению.

Оператор персональных данных работника 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, включая отказ в приеме на работу.

3.3. Работодатель не вправе принимать решения, затрагивающие интересы работника (установление страхового стажа, стажа работы, дающего право на получение надбавки за выслугу лет и т.п.), основываясь на данных, допускающих неоднозначное толкование. Если на основании персональных данных работника невозможно достоверно установить какой-либо факт, работодатель предлагает работнику представить письменные разъяснения.

3.4. Защита персональных данных работников от неправомерного их использования или утраты обеспечиваются работодателем за счет его средств в порядке, установленном Трудовым кодексом Российской Федерации или иными федеральными законами.

IV. Хранение, использование и передача персональных данных работников

4.1. Получение, хранение, анализ, передача или любое другое использование персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по работе, обеспечения личной безопасности работников, контроля качества выполняемой работы и обеспечения сохранности имущества.

4.2. Директор, заместитель директора, начальник отдела комплектования архивными документами, начальник отдела учета сохранности и научно-справочного аппарата, начальник отдела использования архивных документов, лицо, ответственное за организацию работ по охране труда, лицо, ответственное за соблюдение требований пожарной безопасности, лицо, ответственное за ведение воинского учета, организуют хранение и использование персональных данных работников в соответствии с Трудовым кодексом Российской Федерации, федеральным законодательством, настоящим Положением в документированном виде применительно к постановлению Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты».

Главный бухгалтер, бухгалтер 1 категории, инспектор отдела кадров (лицо, ответственное за ведение кадрового делопроизводства), заведующий хозяйством, работник, ответственный за организацию обработки персональных данных и их защиту, организуют хранение и использование персональных данных работников в соответствии с Трудовым кодексом Российской Федерации, федеральным законодательством, настоящим Положением, как в документированном виде, применительно к постановлению Госкомстата Российской Федерации от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», так и с использованием программы «1С: Зарплата и кадры государственного учреждения».

4.3. Хранение персональных данных должно осуществляться в форме, позволяющей определить персональные данные конкретного работника, не дольше, чем того требуют цели их обработки, и они подлежат уничтожению по достижении цели обработки.

После увольнения работника документы, содержащие его персональные данные, хранятся в течение трех лет, затем передаются на хранение в архив.

4.4. Персональные данные работников могут быть представлены на бумажных и машинных носителях. Хранение этих носителей осуществляется в оборудованных для этих целей прочных, запираемых на замки и опечатываемых шкафах.

Размещение, специальное оборудование, организация охраны и режима доступа в помещениях, где ведется работа с персональными данными, производится с учетом необходимости обеспечения сохранности носителей персональных данных работников и средств защиты информации, а также исключения возможности неконтролируемого проникновения или пребывания в них посторонних лиц и просмотра посторонними лицами ведущихся там работ.

4.5. Передача персональных данных в пределах архива:

4.5.1. Право доступа ко всем персональным данным работника имеют директор, заместитель директора.

4.5.2. Право доступа к персональным данным в объеме, необходимом для выполнения ими трудовых функций в соответствии с действующим трудовым законодательством, имеют: главный бухгалтер; бухгалтер 1 категории; инспектор отдела кадров (лицо, ответственное за ведение кадрового делопроизводства); заведующий хозяйством; начальник отдела комплектования архивными документами, начальник отдела учета сохранности и научно-справочного аппарат, начальник отдела использования архивных документов; работник, ответственный за организацию обработки персональных данных и их защиту; лицо, ответственное за организацию работ по охране труда; лицо, ответственное за соблюдение требований пожарной безопасности; лицо, ответственное за ведение воинского учета.

4.5.3. Перечни должностей, имеющих право доступа к персональным данным работников, при исполнении ими должностных обязанностей, связанных с трудовыми функциями, на которых распространяется ответственность по защите персональных данных при их обработке, утверждаются приказом архива.

Учет лиц, имеющих право доступа к персональным данным при их обработке, осуществляется инспектором отдела кадров (лицом, ответственным за ведение кадрового делопроизводства).

4.5.4. Обеспечение конфиденциальности персональных данных не требуется: в случае обезличивания персональных данных; в отношении общедоступных персональных данных.

4.6. Передача персональных данных работника третьим лицам осуществляется с письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью

работника; в рамках трудовых отношений, в том числе связанных с финансово-хозяйственной деятельностью работодателя; в случаях оформления работником банковского кредита, виз и других документов, требующих предоставления справок с места работы, по его письменному заявлению; а также в других случаях, предусмотренных Трудовым кодексом Российской Федерации или федеральными законами. Эти лица должны быть предупреждены о том, что переданные данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

4.7. Ведение количественного и качественного учета и анализа данных о персонале, подготовка статистической отчетности для представления руководству архива оперативной информации, а также для других целей осуществляются при условии обязательного обезличивания персональных данных.

V. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных

5.1. При обработке персональных данных принимаются необходимые организационные и технические меры, в том числе используются криптографические средства для защиты персональных данных от неправомерного или случайного доступа к ним, с целью их уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий с персональными данными.

5.2. Защита персональных данных работников с использованием при их обработке технических средств организуется в соответствии с требованиями действующего законодательства Российской Федерации.

5.3. Организационно-методологическое руководство над работами по обеспечению безопасности персональных данных работников в информационных системах персональных данных работников и осуществление контроля над состоянием их защиты возлагается на лицо, осуществляющее контроль за соблюдением норм защиты информации.

5.4. Безопасность персональных данных при их обработке в информационных системах персональных данных работников организуют и обеспечивают главный бухгалтер, инспектор отдела кадров (лицо, ответственное за ведение кадрового делопроизводства).

5.5. Работы по обеспечению безопасности персональных данных работников при их обработке в информационных системах персональных данных работников являются неотъемлемой частью работ по созданию информационных систем персональных данных работников.

5.6. К объектам защиты относятся:

5.6.1. Автоматизированные рабочие места директора, заместителя директора, начальника отдела комплектования архивными документами, начальника отдела учета сохранности и научно-справочного аппарата, начальника отдела использования архивных документов, работника, лица,

ответственного за работу по охране труда, лица, ответственного за соблюдение требований пожарной безопасности, лица, ответственного за организацию воинского учета, главного бухгалтера, бухгалтера 1 категории, инспектора отдела кадров (лица, ответственного за ведение кадрового делопроизводства), заведующего хозяйством, работника, ответственного за организацию обработки персональных данных и их защиту, а также других лиц, уполномоченных работодателем на обработку и использование персональных данных.

5.6.2. Персональные компьютеры главного бухгалтера, бухгалтера 1 категории, инспектора отдела кадров (лица, ответственного за ведение кадрового делопроизводства), заведующего хозяйством, работника, ответственного за организацию обработки персональных данных и их защиту, а также других лиц, уполномоченных работодателем, с установленным программным обеспечением обработки и хранения персональных данных работников («1С: Зарплата и кадры государственного учреждения» и др.).

5.6.3. Информационные ресурсы, представленные на бумажных и электронных носителях, содержащие персональные данные работников.

5.6.4. Система защиты информации; помещения, в которых размещаются носители или средства обработки персональных данных.

5.7. Технические требования по защите автоматизированных рабочих мест и серверов, используемых при обработке персональных данных работников:

- в качестве операционной системы на автоматизированных рабочих местах директора, заместителя директора, начальника отдела комплектования архивными документами, начальника отдела учета сохранности и научно-справочного аппарата, начальника отдела использования архивных документов, работника, лица, ответственного за организацию работ по охране труда, лица, ответственного за соблюдение требований пожарной безопасности, лица, ответственного за ведение воинского учета, главного бухгалтера, бухгалтера 1 категории, инспектора отдела кадров (лица, ответственного за ведение кадрового делопроизводства), заведующего хозяйством, работника, ответственного за организацию обработки персональных данных и их защиту, а также других лиц, уполномоченных работодателем на обработку и использование персональных данных, устанавливаются версии операционных систем Windows 7, 8, 10;

- применяемые технические средства защиты должны быть сертифицированы по требованиям безопасности;

- для обеспечения обработки информации используются только лицензионные программные средства.

5.8. Эксплуатация автоматизированных рабочих мест директора, заместителя директора, начальника отдела комплектования архивными документами, начальника отдела учета сохранности и научно-справочного аппарата, начальника отдела использования архивных документов, работника, лица, ответственного за организацию работ по охране труда, лица, ответственного за соблюдение требований пожарной безопасности, лица, ответственного за ведение воинского учета, главного бухгалтера, бухгалтера 1

категории, инспектора отдела кадров (лица, ответственного за ведение кадрового делопроизводства), заведующего хозяйством, работника, ответственного за организацию обработки персональных данных и их защиту, а также других лиц, уполномоченных работодателем на обработку и использование персональных данных, осуществляется с обеспечением следующих мер защиты:

- двухфакторная аутентификация пользователей при входе с систему и доступу к защищаемым ресурсам, в том числе с использованием электронных ключей eToken;

- разграничение доступа субъектов к защищаемым ресурсам с использованием операционной системы и аппаратно-программных (программных) средств защиты от НСД;

- обеспечение целостности программных средств, а также неизменности среды;

- копирование защищаемых ресурсов на учтенный локальный машинный носитель;

- обеспечение антивирусной защиты.

5.9. Для обмена персональными данными при их обработке в информационных системах персональных данных и предотвращения перехвата информации в локальной вычислительной сети должны использоваться защищенные каналы связи с применением средств криптографической защиты информации.

VI. Права и обязанности работника в целях защиты своих персональных данных

6.1. Работник имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- подтверждение факта обработки персональных данных;

- правовые основания и цели обработки персональных данных;

- цели и применяемые оператором способы обработки персональных данных;

- наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

- сроки обработки персональных данных, в том числе сроки их хранения;

- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

- иные сведения, предусмотренные федеральными законами.

6.2. Работник вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

6.3. Работник вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

VII. Обязанности работодателя

7.1. Работодатель при обработке персональных данных работника обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении персональных данных.

7.2. Работодатель обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные, если предоставление персональных данных является обязательным в соответствии с федеральным законом.

7.3. Работодатель обязан обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных.

7.4. Оператор обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», субъекту персональных данных информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных либо в течение тридцати дней с даты получения запроса субъекта персональных данных.

7.5. В случае отказа в предоставлении информации о наличии персональных данных оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», или иного федерального закона, являющегося основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных, либо с даты получения запроса субъекта персональных данных.

7.6. Оператор обязан предоставить безвозмездно субъекту персональных данных возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных

сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить субъекта персональных данных о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

7.7. Оператор обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

7.8. В случае выявления неправомерной обработки персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) на период проверки. В случае выявления неточных персональных данных оператор обязан осуществить блокирование персональных данных на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

7.9. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных, или иных необходимых документов, обязан уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.10. В случае выявления неправомерной обработки персональных данных, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

7.11. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее

прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, является субъект персональных данных, или законодательством Российской Федерации.

7.12. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, является субъект персональных данных, или другими федеральными законами.

7.13. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3 - 5 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

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

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника привлекаются к дисциплинарной, материальной, а также к гражданско - правовой, административной, уголовной и материальной ответственности, в порядке, установленном Трудовым кодексом Российской Федерации и федеральным законодательством.

Приложение 2
к приказу Муниципального казенного
учреждения «Муниципальный архив
города Керчи»
от 14 января 2016 года № 8

Перечень должностей работников Муниципального казенного учреждения
«Муниципальный архив города Керчи»,
ответственных за организацию обработки персональных данных работников и
их защиту

| № п/п | Должность или ответственное лицо | Доступ к персональным данным |
|-------|--|---|
| 1 | 2 | 3 |
| 1. | Директор | доступ ко всем персональным данным |
| 2. | Заместитель директора | доступ ко всем персональным данным |
| 3. | Главный бухгалтер | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 4. | Бухгалтер 1 категории | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 5. | Инспектор отдела кадров | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 6. | Заведующий хозяйством | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 7. | Начальник отдела комплектования архивными документами | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 8. | Начальник отдела учета сохранности и научно-справочного аппарата | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 9. | Начальник отдела использования архивных документов | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |

Приложение 3
к приказу Муниципального казенного
учреждения «Муниципальный архив
города Керчи»
от 14 января 2016 года № 8

Перечень должностей работников Муниципального казенного учреждения
«Муниципальный архив города Керчи»,
имеющих право доступа к персональным данным работников,
в том числе в программе «1С: Зарплата и кадры государственного учреждения»,
при исполнении ими должностных обязанностей, связанных с трудовыми
функциями, на которых распространяется ответственность по защите
персональных данных при их обработке

| № п/п | Должность или ответственное лицо | Доступ к персональным данным |
|----------|-------------------------------------|---|
| 1 | 2 | 3 |
| 1. | Главный бухгалтер | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 2. | Бухгалтер 1 категории | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 3. | Инспектор отдела кадров | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 4. | Заведующий хозяйством | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |

Приложение 4
к приказу Муниципального казенного
учреждения «Муниципальный архив
города Керчи»
от 14 января 2016 года № 8

Перечень должностей работников Муниципального казенного учреждения
«Муниципальный архив города Керчи»,
имеющих право доступа к персональным данным работников,
при исполнении ими должностных обязанностей, связанных с трудовыми
функциями, на которых распространяется ответственность по защите
персональных данных при их обработке

| № п/п | Должность или ответственное лицо | Доступ к персональным данным |
|----------|--|---|
| 1 | 2 | 3 |
| 1. | Директор | доступ ко всем персональным данным |
| 2. | Заместитель директора | доступ ко всем персональным данным |
| 3. | Начальник отдела комплектования архивными документами | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 4. | Начальник отдела учета сохранности и научно-справочного аппарата | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |
| 5. | Начальник отдела использования архивных документов | доступ к персональным данным работников в объеме, необходимом для выполнения трудовых функций |

Приложение 5
к приказу Муниципального казенного
учреждения «Муниципальный архив
города Керчи»
от 14 января 2016 года № 8

Перечень лиц, ответственных за охрану труда, пожарную безопасность, воинский учет в Муниципальном казенном учреждении «Муниципальный архив города Керчи», имеющих право доступа к персональным данным работников при выполнении возложенных обязанностей, на которых распространяется ответственность по защите персональных данных при их обработке

| № п/п | Должность или ответственное лицо | Доступ к персональным данным |
|-------|--|---|
| 1 | 2 | 3 |
| 1. | Лицо, ответственное за организацию работ по охране труда | доступ к персональным данным работников в объеме, необходимом для выполнения возложенных обязанностей |
| 2. | Лицо, ответственное за соблюдение требований пожарной безопасности | доступ к персональным данным работников в объеме, необходимом для выполнения ими возложенных обязанностей |
| 3. | Лицо, ответственное за ведение воинского учета | доступ к персональным данным работников в объеме, необходимом для выполнения ими возложенных обязанностей |