Утверждаю
Председатель первичной
профсоюзной организации МБУ
«Шумячский музей»
_____ С.Н.Семенова

Приложение к приказу муниципального бюджетного учреждения «Шумячский художественно-краеведческий музей» Шумячского района Смоленской области от 11.11.2016г. № 9

ПОЛОЖЕНИЕ
по обеспечению безопасности персональных данных в муниципальном бюджетном учреждении «Шумячский художественно-краеведческий музей» Шумячского района Смоленской области

1. Общие положения

1.1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных работников муниципального бюджетного учреждения «Шумячский художественно-краеведческий музей» Шумячского района Смоленской области (далее – учреждение) при их обработке, в том числе в информационных системах, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

1.2. Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных» и определяет порядок обработки и защиты персональных данных работников учреждения.

1.3. Персональные данные работника - любая информация, относящаяся к данному работнику (субъекту персональных данных) и необходимая учреждению в связи с трудовыми отношениями, в том числе:

фамилия, имя, отчество работника;

дата и место рождения работника;

адрес работника;

семейное, социальное, имущественное положение работника;

образование, профессия работника;

доходы, имущество и имущественные обязательства работника;

другая аналогичная информация, на основании которой возможна безошибочная идентификация субъекта персональных данных.

- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях или дополнениях;

- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

10. Обязанности работников по обеспечению достоверности его персональных данных

Работники должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области. Работник должен быть заранее предупрежден о необходимости предоставления достоверных сведений и о возможности ответственности в случае нарушения своей обязанности.

11. Порядок передачи информации о работнике

К передаче информации о работнике относятся запросы о получении информации о работниках учреждения, направленные различными государственными органами, в том числе из судебных или правоохранительных органов.

На основании части 2 статьи 57 Гражданского процессуального кодекса Российской Федерации (ГПК РФ) суд вправе выдать работнику запрос для получения доказательства или направить запрос самостоятельно.

В ситуациях, когда предоставление сведений о персональных данных работника может потребоваться при ведении расследования по уголовным делам, статьей 21 Уголовно-процессуального кодекса Российской Федерации (УПК РФ) предусмотрено, что запросы прокурора, следователя, органа дознания и дознавателя, предъявленные в пределах их полномочий, установленных УПК РФ, обязательны для исполнения всеми учреждениями, предприятиями, организациями, должностными лицами и гражданами.

12. Ответственность за нарушение законодательства об охране персональных данных

12.1. Работники учреждения, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

12.2. Руководитель учреждения за нарушение порядка обращения с персональными данными несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях РФ, а также возмещает сотруднику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные об этом сотруднике.

Приложение № 1
к Положению по обеспечению безопасности персональных данных в муниципальном бюджетном учреждении «Шумячский художественно-краеведческий музей» Шумячского района Смоленской области

Персональные данные работников
муниципального бюджетного учреждения
«Шумячский художественно-краеведческий музей»
Шумячского района Смоленской области

- фамилия, имя, отчество;
- паспортные данные;
- год, месяц, дата и место рождения, а также иные данные, содержащиеся в удостоверении личности работника;
- гражданство;
- данные о семейном, социальном и имущественном положении;
- данные об образовании работника, наличии специальных знаний или подготовки;
- данные о профессии, специальности работника;
- сведения о доходах работника;
- данные медицинского характера, в случаях, предусмотренных законодательством;
- данные о членах семьи работника;
- данные о месте жительства, почтовый адрес, телефон работника, а также членов его семьи;
- данные, содержащиеся в трудовой книжке работника и его личном деле, страховом свидетельстве государственного пенсионного страхования, свидетельстве о постановке на налоговый учет;
- данные, содержащиеся в документах воинского учета (при их наличии);
- Документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям (об инвалидности, ... к труду.... и т.п.)
- иные персональные данные.

1.4. Сведения о персональных данных работников относятся к числу конфиденциальных (составляющих охраняемую законом тайну учреждения). Режим конфиденциальности в отношении персональных данных снимается:

в случае их обезличивания;

по истечении 75 лет срока их хранения;

в других случаях, предусмотренных федеральными законами.

2. Основные понятия

2.1. Для целей настоящего Положения используются следующие основные понятия:

персональные данные работника - в соответствии с определением п. 1.3 настоящего Положения;

обработка персональных данных работника - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

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 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 уполномоченным должностным лицом училища 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.

3. Перечень документов, в которых содержатся сведения, составляющие персональные данные Работников

- документы, предъявляемые работником при заключении трудового договора, в том числе:

паспорт или иной документ, удостоверяющий личность;

трудовая книжка, за исключением случаев, когда договор заключается впервые или работник поступает на работу на условиях совместительства, или трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;

страховое свидетельство государственного пенсионного страхования;

документы воинского учета – для лиц, подлежащих воинскому учету;

документ об образовании, о квалификации или наличии специальных знаний при поступлении на работу, требующую специальных знаний или специальной подготовки;

свидетельство о присвоении ИНН (при его наличии у работника).

- документы о составе семьи работника, необходимые для предоставления гарантий, связанных с выполнением семейных обязанностей (например: свидетельство о заключении брака, свидетельство о рождении детей);

- документы о состоянии здоровья детей и других близких родственников (например: справки об инвалидности), когда с наличием таких документов связано предоставление работнику каких-либо гарантий и компенсаций;

- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (об инвалидности, ограничении к труду в определенных условиях, донорстве, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т.п.).

Перечень персональных данных работников представлен в приложении № 1.

4. Принципы обработки персональных данных и условия проведения сбора и обработки персональных данных

К основным принципам обработки персональных данных относятся:

а) принцип законности целей и способов обработки персональных данных;

б) принцип соответствия объема и характера обрабатываемых персональных данных, способов их обработки и целям обработки персональных данных;

в) принцип достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к заявленным при их сборе целям;

г) принцип недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

д) принцип защиты персональных данных от неправомерного доступа и их использования или утраты.

При обработке персональных данных должны соблюдаться следующие общие требования согласно положению статьи 86 Трудового кодекса РФ:

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 и обеспечения сохранности имущества;

2) при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом РФ и иными федеральными законами;

3) все персональные данные работника 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 и последствиях отказа работника дать письменное согласие на их получение;

4) 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 и обрабатывать данные о частной жизни работника только с его письменного согласия;

5) работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его

профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом РФ или иными федеральными законами;

6) при принятии решений, затрагивающих интересы работника, работодатель не имеет право основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;

7) защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ или иными федеральными законами;

8) работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работником, а также об их правах и обязанностях в этой области;

9) работники не должны отказываться от своих прав на сохранение и защиту тайны;

10) работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

5. Работа с документами, содержащими персональные данные работника.

Персональные данные работника содержатся в основном документе персонального учета работников – в личной карточке работника, которая заполняется сотрудником кадровой службы после издания приказа о его приеме на работу и хранится в специально оборудованном шкафу.

Для уничтожения данных на бумажных носителях в учреждении, работающем с персональными данными работников, или в отдельно стоящем помещении должна быть установлена офисная техника «Уничтожение документов».

6. Хранение и использование персональных данных работников

Документы, содержащие информацию о персональных данных работника хранятся на бумажном и электронном носителе в кадровой службе учреждения и бухгалтерии. Доступ к такой информации без получения специального разрешения имеют директор учреждения и главный бухгалтер. Иные работники учреждения могут иметь доступ к персональным данным работников в случае, если они получили разрешение директора в виде визы на служебной записке, обосновывающей необходимость ознакомления и использования персональных данных конкретного работника.

Со сторонними работниками, сопровождающими работу информационных систем, заключается договор о неразглашении персональных данных работников.

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

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Работа по обеспечению безопасности персональных данных при их обработке в информационных системах является неотъемлемой частью работ по созданию информационных систем.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

Размещение информационных систем, специальное оборудование и охрана помещений (с помощью систем сигнализации), в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения в этих помещениях посторонних лиц.

При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с

использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) организация учета лиц, допущенных к работе с персональными данными в информационной системе на основании служебных записок и дополнительных трудовых соглашений;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании пункта 6 данного Положения.

Контроль за организацией доступа к персональным данным возлагается на директора учреждения и главного бухгалтера.

При обнаружении нарушений порядка предоставления персональных данных ответственные незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

8. Передача персональных данных работников

При передаче персональных данных работников учреждения ответственные работники должны 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 других случаях, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами;

- 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 секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном ТК РФ и иными федеральными законами;

- осуществлять передачу персональных данных работника в пределах учреждения в соответствии с локальным нормативным актом, с которым работник должен быть ознакомлен под роспись;

- 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 иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

9. Права работников в области защиты персональных данных

В целях обеспечения защиты персональных данных, хранящихся у работодателя, работники имеют право на:

- полную информацию об их персональных данных и обработке этих данных;

- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных федеральным законом;

- определение своих представителей для защиты своих персональных данных;

- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований ТК РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия.