



УТВЕРЖДАЮ

Директор

МБУК «Центр культуры» НГО

В.П. Нестеренко

« 30 » декабря 2015 г.

Положение о защите персональных данных работников МБУК «Центр культуры» НГО

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статьи Конституции Российской Федерации, Трудового кодекса РФ, кодекса об административных правонарушениях РФ, Гражданского кодекса РФ, Уголовного кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации».

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается обезличивания или истечения 75 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом директора и является для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

2.1. Персональные данные работника – информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника входят:

- фамилия, имя, отчество,
- дата и место рождения,
- адрес места жительства,
- данные документа, удостоверяющего личность,
- идентификационный номер налогоплательщика,
- данные свидетельства государственного пенсионного страхования,
- данные об образовании,
- сведения о трудовом и общем стаже,
- сведения о составе семьи,
- сведения о воинском учете,
- сведения о заработной плате сотрудника,
- сведения о социальных льготах,
- специальность,
- занимаемая должность,
- наличие судимостей,
- табельный номер,

- контактные данные (номер телефона, факса, адрес электронной почты),
- данные свидетельства о государственной регистрации акта гражданского состояния,
- номер лицевого счета,
- содержание трудового договора,
- подлинники и копии приказов по личному составу,
- личные дела и трудовые книжки сотрудников.

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

3. Обработка персональных данных

3.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое использование персональных данных работника.

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

- при определении объема и содержания, обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом и иными федеральными законами,
- получение персональных данных осуществляется путем представления их самим работником,
- работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника могут быть получены и обработаны работодателем только с его письменного согласия,
- работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом,

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:

- бухгалтерии,
- отдела кадров.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законом.

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

3.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом,

- не сообщать персональные данные работника в коммерческих целях без его письменного согласия,
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, должны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами,
- разрешить доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по Учреждению, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций,
- запрашивать сведения о состоянии здоровья работника, которые относятся к вопросу о возможности выполнения работником трудовой функции,

3.5.2 Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

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

3.7. Не допускается распространение персональной информации по телефону или факсу.

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

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри учреждения).

4.1.1. Право доступа к персональным данным сотрудника имеют:

- директор учреждения,
- руководитель структурного подразделения,
- при переводе из одного структурного подразделения в другое, доступ к персональным данным сотрудника может иметь руководитель нового подразделения,
- сам работник,
- другие сотрудники организации при выполнении ими служебных обязанностей.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом директора учреждения.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:

- налоговые инспекции,
- правоохранительные органы,
- органы статистики,
- военкоматы,
- органы социального страхования,
- пенсионные фонды,
- подразделения муниципальных органов управления.

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Другие организации.

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

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника. В случае развода бывшая супруга (супруг) имеют право обратиться в учреждение с письменным запросом о размере заработной платы сотрудника без его согласия согласно Уголовного кодекса РФ.

5. Защита персональных данных

5.1. Под угрозой утраты персональных данных понимается любое проявление злоумышленных возможностей, внешних или внутренних источников угрозы, создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. 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.

5.3. Защита персональных данных представляет собой жестко регламентированный процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности учреждения.

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

5.5. «Внутренняя защита».

5.5.1. Регламентация доступа персонала к персональным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами учреждения.

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

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
 - строгое обоснованное распределения документов и информации между работниками;
 - рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
 - знание работником требований нормативно-методических указаний 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 в помещение, в котором находятся средства, содержащие конфиденциальную информацию;
 - организация порядка уничтожения информации;
 - разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
 - не допускается выдача личных дел работников на рабочие места руководителей.
- Ознакомиться с личным делом можно в кабинете Отдела кадров.
- не допускается выносить личные дела работников за пределы учреждения.

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Все электронные документы, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается сотрудникам Отдела кадров, руководителю учреждения.

5.6. «Внешняя защита».

5.6.1. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в Отделе кадров учреждения.

5.6.2. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим учреждения;
- технические средства охраны, сигнализации;
- порядок охраны территории, здания, помещений.

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

5.8. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут разработать свои совместные меры защиты персональных данных работников.

6. Права и обязанности работника

6.1. Закрепление прав работников, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

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

6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных,
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные;
- на сохранение и защиту своей личной и семейной тайны.

6.4. Работник обязан:

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

6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, образовании, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные о профессии, специальности, присвоении нового разряда и пр.

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

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

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут

ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником возложенных на него обязанностей по соблюдению порядка работы с конфиденциальными сведениями работодатель вправе применить, предусмотренные Трудовым кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудников, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права свободы. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо предоставление неполной или заведомо ложной информации – влечет наложение на должностных лиц административного штрафа.