#  Утверждено приказом

# МБУК «Дом молодежи» НГО

 от 05.11.2019 г. № 157

**Положение**

**о порядке обработки, хранении и использовании персональных данных работников Муниципального бюджетного учреждения культуры «Дом молодежи» Находкинского городского округа и гарантии их защиты**

1. **Общие положения**

1.1. Настоящее положение является локальным правовым актом Муниципального бюджетного учреждения культуры «Дом молодежи» Находкинского городского округа (далее – учреждение), являющимся оператором персональных данных.

1.2. Настоящее положение устанавливает порядок осуществления операций с персональными данными сотрудников учреждения.

1.3. Настоящее положение разработано в целях:

- регламентации порядка осуществления операций с персональными данными сотрудников учреждения;

- обеспечения требований закона № 152-ФЗ и иных правовых актов, регулирующих использование персональных данных;

- установления прав и обязанностей сотрудников учреждения в части работы с персональными данными;

- установления механизмов ответственности сотрудников учреждения за нарушение локальных норм, а также положений федерального, регионального и муниципального законодательства, регулирующих использование персональных данных.

1.4. Настоящее положение вступает в силу в момент его утверждения отдельным приказом директора учреждения и действует бессрочно до замены новым локальным правовым актом аналогичного назначения.

1.5. Корректировка настоящего положения осуществляется отдельными приказами директора учреждения.

1.6. Все сотрудники учреждения должны быть ознакомлены с настоящим положением под роспись.

1.7. Ограничение несанкционированного доступа к персональным данным обеспечивается учреждением и снимается в момент их обезличивания, а также по истечении 75 лет их хранения, если иное не установлено законом или решением руководства учреждения.

1.8. Основным инфраструктурным ресурсом учреждения для осуществления операций с персональными данными являются информационные системы, представляющие собой:

- комплексы автоматизированной обработки персональных данных (позволяющих осуществлять операции с персональными данными в виде файлов, доступ к которым регулируется в соответствии с положениями локальных правовых актов учреждения, федеральных, региональных и муниципальных НПА);

- документацию на бумажных носителях (доступ к которым также осуществляется в соответствии с положениями локальных правовых актов и законодательства РФ).

1. **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:

- все биографические сведения работника (фамилия, имя, отчество, дата рождения, место рождения, гражданство);

- образование;

- специальность,

- занимаемая должность;

- стаж работы;

- наличие судимостей;

- знание иностранных языков;

- сведения о наградах, достижениях (заслугах);

- адрес места жительства (по паспорту и фактический), дата регистрации по указанному месту жительства;

- телефоны;

- состояние в браке;

- состав семьи;

- идентификационный номер налогоплательщика;

- данные страхового свидетельства обязательного пенсионного страхования;

- размер заработной платы;

- сведения о воинском учете;

- подлинники и копии приказов по личному составу;

- личные дела, личные карточки (форма Т2) и трудовые книжки работников;

- основания к приказам по личному составу;

- дела, содержащие материалы по повышению квалификации и переподготовке работников, служебным расследованиям;

- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;

- фотографии.

 2.3. Специалист по персоналу обеспечивает проверку вышеперечисленных документов, содержащих персональные данные сотрудников, на предмет подлинности, а также обеспечивает при необходимости их временное хранение в установленном порядке.

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

1. **Обработка персональных данных**

3.1. Настоящее положение устанавливает, что учреждение осуществляет следующие операции с персональными данными работников:

- получение;

- обработка;

- передача;

- блокирование;

- хранение;

- ликвидация.

3.2. Под получением персональных данных понимается последовательность действий, связанных с установлением достоверности соответствующих данных, а также размещением их в информационных системах учреждения.

3.2. Под обработкой персональных данных понимается прочтение, корректировка или дополнение соответствующих данных, совершаемые уполномоченным лицом учреждения.

3.3. Под передачей персональных данных понимается операция:

- по адресному размещению соответствующих данных на носителях и серверах, доступ к которым имеют сотрудники учреждения либо третьи лица;

- по размещению персональных данных в источниках внутрикорпоративного документооборота;

- по опубликованию в интересах учреждения персональных данных о работнике в СМИ или на серверах интернета в соответствии с нормами законодательства.

3.4. Под блокированием персональных данных понимается временный запрет на осуществление каких-либо операций с персональными данными, которые находятся в информационных системах учреждения, в случаях, предусмотренных положениями локальных правовых актов учреждения и законодательства РФ.

3.5. Под хранением персональных данных понимается совокупность операций, направленных на обеспечение целостности соответствующих данных посредством их размещения в информационных системах учреждения.

3.6. Под ликвидацией персональных данных понимается операция по изъятию соответствующих данных из информационных систем учреждения, а также обеспечению невозможности их восстановления.

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

 3.7.1. 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.

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

3.8.1. 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 данных 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 доступ к персональным данным 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 по учреждению, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций,

- запрашивать только те сведения о состоянии здоровья работника, которые относятся к вопросу выполнения им трудовой функции.

3.8.2 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.

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

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

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

**4. Порядок осуществления операций с персональными данными**

4.1. Получение персональных данных (документов, на которых они зафиксированы) осуществляется непосредственно от сотрудника учреждения. В случае если предоставление соответствующих данных возможно только от третьих лиц, то сотрудник должен дать письменное согласие на это.

4.2. Учреждение не имеет права требовать и получать персональные данные сотрудника, отражающие личные аспекты его жизни, религиозные, политические, философские взгляды.

4.3. Обработка персональных данных сотрудника может осуществляться только с его письменного согласия (Приложение № 1 к настоящему положению) за исключением тех случаев, что предусмотрены подп. 2-11 п. 1 ст. 6 закона от 27.07.2006 «О персональных данных» № 152-ФЗ.

4.4. Передача персональных данных сотрудника осуществляется по защищенным каналам связи, при задействовании средств криптозащиты, а также осуществляется посредством перемещения или копирования содержимого данных носителей при участии уполномоченных сотрудников учреждения.

4.5. Блокирование данных осуществляется посредством закрытия доступа к файлам при задействовании средств криптозащиты, а также посредством закрытия доступа к соответствующей информационной системе для определенных групп сотрудников.

4.6. Хранение данных осуществляется на персональном компьютере специалиста по персоналу, на облачных серверах и в архиве учреждения.

4.7. Ликвидация персональных данных осуществляется посредством их удаления с персонального компьютера специалиста по персоналу, серверов и посредством уничтожения других соответствующих носителей.

**5. Организация доступа к персональным данным**

5.1. Внутренний доступ (доступ внутри учреждения) к персональным данным сотрудников учреждения, не требующий подтверждения и не подлежащий ограничению, имеют:

- директор учреждения;

- заместитель директора учреждения;

- сотрудники бухгалтерии учреждения;

- специалист по персоналу;

- руководители структурных подразделений (доступ к персональным данным только работников своего подразделения).

5.2. Доступ к персональным данным сотрудников учреждения для иных лиц может быть разрешен только отдельным распоряжением директора.

5.3. Внешний доступ к персональным данным сотрудников учреждения имеют:

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

- налоговые инспекции,

- правоохранительные органы,

- органы статистики,

- военкоматы,

- органы социального страхования,

- пенсионные фонды,

 - подразделения муниципальных органов управления.

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

5.3.3. 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.

1. **Защита персональных данных**
	1. Под угрозой утраты персональных данных понимается любое проявление злоумышленных возможностей, внешних или внутренних источников угрозы, создающее неблагоприятные события, оказывающее дестабилизирующее воздействие на защищаемую информацию.
	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.
	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.
	4. Защита персональных данных работника от неправомерного использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.
	5. «Внутренняя защита».

6.5.1. 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.

6.5.2. 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 выносить личные дела работников за пределы учреждения.

6.6. Защита персональных данных сотрудника на электронных носителях.

Все электронные документы, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается специалисту по персоналу, работникам бухгалтерии, директору учреждения, его заместителю.

* 1. «Внешняя защита».

6.6.1. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов учреждения, содержащих персональные данные.

6.6.2. 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.

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

1. **Права и обязанности работника**
	1. Закрепление прав работников, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.
	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.
	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.

7.4. 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.

7.5. 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.

1. **Ответственность за разглашение конфиденциальной информации, связанной с персональными данными**
	1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.
	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.
	3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.
	4. Каждый сотрудник учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность информации.
	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.

8.5.1. 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.

8.5.2. 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.

Специалист по персоналу Я.А. Казакова