Муниципальное автономное учреждение
«Хозяйственно-эксплуатационная контора»

УТВЕРЖДАЮ
Начальник МАУ «ХЭК»
_____ А.В. Човган
«__» _____ 2019 г.

ПОЛОЖЕНИЕ
о персональных данных работников

1. Общие положения.

1.1.Настоящим Положением регулируются отношения, связанные с обработкой персональных данных, осуществляемой муниципальным автономным учреждением «Хозяйственно-эксплуатационная контора» (далее – МАУ «ХЭК»), с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных.
1.2.Применяемые в настоящем Положении понятия означают:
1.2.1.**Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
1.2.2.**Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
1.2.3.**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;
1.2.4.**Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;
1.2.5.**Распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;
1.2.6.**Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;
1.2.7.**Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);
1.2.8.**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;
1.2.9.**Обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;
1.2.10.**Информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
1.2.11.**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;
1.2.12.**Использование персональных данных** – действия (операции) с персональными данными, совершаемые должностным лицом Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
1.2.13.**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.

2.Цель

2.1.Целью Положения об обработке персональных данных работников (далее – Положение) является защита персональных данных работников муниципального автономного учреждения «Хозяйственно-эксплуатационная контора» (далее – Учреждение) от несанкционированного доступа, неправомерного их использования или утраты, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.
2.2.Положение разработано в соответствии со статьями 85-90 Трудового Кодекса Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», Правилами внутреннего трудового распорядка Учреждения.
2.3.Порядок ввода в действие и изменения Положения.
2.3.1.Положение вступает в силу с момента утверждения его начальником муниципального автономного учреждения «Хозяйственно-эксплуатационная контора» и действует бессрочно, до замены его новым положением.
2.3.2.Все изменения в Положения вносятся соответствующим приказом.
2.4.Все работники Учреждения должны быть ознакомлены с настоящим Положением под подпись.
2.5.Режим конфиденциальности персональных данных снимается в случае их обезличивания и по истечении 75 лет срока их хранения, или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено законом.

3.Состав персональных данных работников.

3.1.В состав персональных данных работников Учреждения входят:
- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей;
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики.

3.2 Данные документы являются конфиденциальными, при этом, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

4.Обработка персональных данных.

4.1.В целях обеспечения прав и свобод работника Учреждение при обработке персональных данных работника обязаны соблюдать следующие общие требования:
4.1.2.Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.
4.1.3.При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.
4.1.4.Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.
4.1.5.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, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.
4.1.6.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.
4.2.К обработке, передаче и хранению персональных данных работника могут иметь доступ сотрудники:
-Начальник Учреждения;
-Главный бухгалтер;
-Бухгалтер;
-Делопроизводитель.
4.3.Использование персональных данных возможно только в соответствии с целями, определившими их получение.
4.4.Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда работникам МАУ «ХЭК», затруднения реализации прав и свобод. Ограничение прав на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.
4.5.Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.
4.6.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, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;

-разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом Учреждения, 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 Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

4.7.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.

4.8.При передаче персональных данных работника (в том числе и в коммерческих целях) за пределы Учреждения работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

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

4.10.Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

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

4.12.При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

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

5.1.Информация, представляемая работником при поступлении на работу в Учреждение, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт гражданина Российской Федерации;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета — для военнообязанных и 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.

5.2.При оформлении работника в Учреждение заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:

-общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
-сведения о воинском учете;
-данные о приеме на работу;
В дальнейшем в личную карточку вносятся:
-сведения о переводах на другую работу;
-сведения об аттестации;
-сведения о повышении квалификации;
-сведения о профессиональной переподготовке;
-сведения о наградах (поощрениях), почетных званиях;
-сведения об отпусках;
-сведения о социальных гарантиях;
-сведения о месте жительства и контактных телефонах.
5.3.В Учреждении создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:
5.3.1.Документы, содержащие персональные данные работников:
-комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;
-комплекс материалов по анкетированию, тестированию;
-документы по проведению собеседований с кандидатом на должность;
-подлинники и копии приказов по личному составу;
-личные дела и трудовые книжки работников;
-дела, содержащие основания к приказу по личному составу;
-дела, содержащие материалы аттестации работников;
-служебных расследований;
-справочно-информационный банк данных по персоналу (картотеки, журналы);
-подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, руководителям структурных подразделений;
-копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;
5.3.2Документация по организации работы структурных подразделений:
-положения о структурных подразделениях, должностные инструкции работников, приказы, распоряжения, указания руководства Учреждения;
-документы по планированию, учету, анализу и отчетности в части работы с персоналом в Учреждении.

6.Доступ к персональным данным.

6.1.Внутренний доступ (доступ внутри Учреждения).
6.1.1.Право доступа к персональным данным сотрудника имеют:
-Начальник Учреждения;
-Главный бухгалтер;
-Бухгалтер
-Делопроизводитель Учреждения;
-Руководители подразделений по направлению деятельности (доступ к личным данным только сотрудников своего подразделения);
-При переводе из одного структурного подразделения в другое доступ к персональным данным сотрудника может иметь руководитель нового подразделения;
-Сам работник, носитель данных.
-Другие сотрудники Учреждения при выполнении ими своих должностных обязанностей.
6.1.2.Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом начальника Учреждения.

6.2.Внешний доступ.

6.2.1.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;

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

6.2.3.Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

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

6.2.5.Персональные данные сотрудника могут быть представлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

7.Защита персональных данных

7.1.Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Учреждения.

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

7.3.Внутренняя защита.

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

-ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данным сотрудников;

-строгое избирательное и обоснованное распределение документов и информации между работниками;

-рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;

-знание работником требований нормативно – методических документов по защите информации и сохранении тайны;

-наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

-определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

-организация порядка уничтожения информации;

-своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

-разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

-не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только начальнику Учреждения, делопроизводителем и в исключительных случаях, по письменному разрешению начальника Учреждения, руководителю структурного подразделения. (например, при подготовке материалов для аттестации работника).

7.3.2.Защита персональных данных сотрудников на электронных носителях.

7.3.2.1.Все папки, содержащие персональные данные сотрудника, должны иметь ограниченный доступ (только для делопроизводителя).

7.4.Внешняя защита.

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

-порядок приема, учета и контроля деятельности посетителей;

-технические средства охраны (электронный ключ, сигнализации);

-порядок охраны территории, зданий, помещений, транспортных средств;

7.5.Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны не разглашать персональные данные работников.

7.6.Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

8.Права и обязанности работника.

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

8.2.В целях защиты персональных данных, хранящихся в Учреждении, работник имеет право:

-требовать исключения или исправления неверных или неполных данных;

-получать свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные.

-персональные данные оценочного характера дополнить заявлением, содержащим его собственную точку зрения;

-определять своих представителей для защиты своих персональных данных;

-на сохранение и защиту своей личной жизни и семейной тайны.

8.3.Работник обязан передавать Учреждению комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым Кодексом РФ, а также своевременно сообщать об изменениях своих персональных данных.

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

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

9.1.Начальник Учреждения, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

9.2.Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

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

10. Блокирование и уничтожение персональных данных, содержащихся в машинных носителях информации

10.1.Блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях:
-если персональные данные являются неполными, устаревшими, недостоверными;
-если сведения являются незаконно полученными или не являются необходимыми для заявленной оператором персональных данных цели обработки.
10.2. В случае подтверждения факта недостоверности персональных данных уполномоченное Оператором лицо на основании документов, представленных субъектом персональных данных, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязано уточнить персональные данные и снять их блокирование.
10.3. В случае выявления неправомерных действий с персональными данными уполномоченное Оператором лицо обязано устранить (организовать устранение) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожить персональные данные.
10.4. Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное Оператором лицо обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.
10.5.Уполномоченное Оператором лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:
-достижения цели обработки персональных данных оператор;
-отзыва субъектом согласия на обработку своих персональных данных.
10.6. Уничтожение персональных данных должно быть осуществлено в течение трех дней с указанных моментов. В согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных. Уполномоченное Оператором лицо должно направить уведомление о факте уничтожения персональных данных субъекту персональных данных.

11. Работа с бумажными носителями (документами)

11.1.Виды и периоды уничтожения бумажных носителей, содержащих персональные данные, представлены в Приложение 1.
12.2.По окончании срока хранения документы, уничтожаются путём измельчения на мелкие части (или иным способом), исключающие возможность последующего восстановления информации.

12. Работа с машинными носителями информации

12.1.Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее – НЖМД) и машинных носителях: компакт дисках (далее – CD-R/RW, DVD-R/RW в зависимости от формата), FLASH-накопителях. (Приложение 2)
12.2. Машинные носители информации (за исключением НЖМД), перечисленные должны находиться в сейфе, опечатываемом печатью ответственного сотрудника (кроме формируемых или обрабатываемых в данный момент на рабочем месте).
12.3. По окончании указанных сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путём деформирования, нарушения единой целостности носителя или его сжигания.

12.4. Подлежащие уничтожению файлы, расположенные на жестком диске ПЭВМ, удаляются средствами операционной системы с последующим «очищением корзины».
12.4. В случае допустимости повторного использования носителя формата, CD-RW, DVD-RW, FLASH применяется программное удаление («затирание») содержимого диска путём его форматирования с последующей записью новой информации на данный носитель.

13. Порядок оформления документов об уничтожении носителей

13.1.Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя Оператора. Комиссию возглавляет руководитель Оператора (или иное уполномоченное лицо). В состав Комиссии должен входить сотрудник отдела автоматизированных информационных систем и руководитель соответствующего подразделения Оператора.
13.2. В ходе процедуры уничтожения персональных данных носителей необходимо присутствие членов Комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации, находящейся на технических средствах.
13.3. Комиссия составляет и подписывает Акт (2 экземпляра) об уничтожении носителей. В течение трёх дней после составления акты об уничтожении направляются на утверждение руководителю Оператора. После утверждения один экземпляр Акта хранится в сейфе у руководителя соответствующего подразделения Оператора, второй экземпляр Акта хранится у руководителя службы информационной безопасности Оператора.
13.4.Факт уничтожения носителя с персональными данными фиксируется в «Журнале регистрации носителей информации, содержащих персональные данные и иную конфиденциальную информацию», где в графе «Дата и номер акта уничтожения» заносятся соответствующие данные. Данный журнал является документом конфиденциального характера и вместе с актами уничтожения хранится в сейфе.