МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«Административно – хозяйственная служба»

ПРИКАЗ

26.05.2025 № 55

ЗАТО Свободный

Об утверждении и введении в действие Положения «О работе с персональными данными сотрудников», Положения «О защите персональных данных», Положения «О порядке уничтожения персональных данных», Положения «О внутреннем контроле работы с персональными данными», Регламента «О допуске работников к обработке персональных данных третьих лиц» в МКУ «Административно-хозяйственная служба»

В целях исполнения требований главы 14 Трудового кодекса «Зашиты персональных данных работника», Федерального закона от 27.07.2006 года № 152-ФЗ «О персональных данных», постановления Правительства от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и постановления Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных при их обработке в информационных системах персональных данных» при обработке персональных данных в МКУ «Административно-хозяйственная служба»

ПРИКАЗЫВАЮ:

1. Утвердить Положение «О работе с персональными данными сотрудников» МКУ «Административно-хозяйственная служба» и ввести в действие с 26 мая 2025 года (Приложение № 1).
2. Утвердить Положение «О защите персональных данных» в МКУ «Административно-хозяйственная служба» (Приложение № 2).
3. Утвердить и ввести Положение «О порядке уничтожения персональных данных» в МКУ «Административно-хозяйственная служба» (Приложение № 3).
4. Утвердить Положение «О внутреннем контроле работы с персональными данными» МКУ «Административно-хозяйственная служба» (Приложение № 4).

5. Утвердить Регламент «О допуске работников к обработке персональных данных третьих лиц» в МКУ «Административно-хозяйственная служба» (Приложение № 5).

6. Делопроизводителю Носивской Ю.Э. ознакомить всех сотрудников МКУ «Административно-хозяйственная служба» под подпись с положениями о работе и защиты с персональными данными.

7. Контроль за исполнением настоящего приказа оставляю за собой.

И.о. директора МКУ
«Административно-хозяйственная служба» А.А. Кузнецов

Ознакомлены:

_____ А.Н. Руденко

_____ М.В. Орехова

_____ Ю.Э. Носивская

_____ К.А. Беседина

_____ М.С. Газиева

_____ К.В. Усанова

_____ В.Л. Соболь

_____ В.Ю. Бем

_____ В.Е. Васькова

_____ В.Н. Дунаев

_____ Т.Н. Дунаева

_____ И.Ю. Ерофеев

_____ М.Н. Путилов

_____ С.В. Татаринцев

_____ В.А. Селиверстов

_____ Д.А. Кузнецов

_____ А.Г. Якубов

Приложение № 1

УТВЕРЖДАЮ
И. о. директора МКУ
«Административно-хозяйственная служба»
_____ А.А. Кузнецов
«26» 05 2025 г.

ПОЛОЖЕНИЕ
о работе с персональными данными сотрудников

1. Общие положения

1.1. Положение о работе с персональными данными сотрудников МКУ «Административно-хозяйственная служба» разработано в соответствии с Трудовым кодексом РФ, Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и нормативно-правовыми актами, действующими на территории России.

1.2. Настоящее Положение определяет порядок работы (сбора, обработки, использования, хранения и т. д.) с персональными данными сотрудников и гарантии конфиденциальности сведений о сотруднике, предоставленных сотрудником работодателю.

1.3. Настоящее Положение вступает в силу с 26 мая 2025 года.

2. Получение и обработка персональных данных сотрудников

2.1. Персональные данные сотрудника работодатель получает непосредственно от сотрудника. Работодатель вправе получать персональные данные сотрудника от третьих лиц только при наличии письменного согласия сотрудника или в иных случаях, прямо предусмотренных в законодательстве.

2.2. В состав персональных данных, которые работник сообщает работодателю, входят:

- фамилия, имя, отчество;
– пол;
– дату рождения;
- место рождения;
- возраст;
- гражданство;

– отношение к воинской обязанности;
– местожительство и домашний (сотовый) телефон;
– образование, специальность;
– предыдущее (ие) место (а) работы;
- сведения об образовании;
- адрес места проживания;
- паспортные данные;
- сведения о воинском учете;
- страховой номер индивидуального лицевого счета;
- сведения о трудовой деятельности;
- сведения о семейном положении;
- специальные персональные данные: сведения о судимости, сведения о состоянии здоровья;
- иные сведения, которые относятся к трудовой деятельности работника.

2.3. Работодатель не вправе требовать от сотрудника предоставления информации о политических и религиозных убеждениях, о его частной жизни, членстве в общественных объединениях или профсоюзной деятельности.

2.4. Сотрудник предоставляет работодателю достоверные сведения о себе. Работодатель проверяет достоверность сведений, сверяя данные, предоставленные сотрудником, с имеющимися у сотрудника документами.

2.5. Сотрудник в целях своевременной актуализации сведений в кадровых документах, получения гарантий и компенсаций, установленных законом или локальными актами организации, а также сдачи Работодателем корректной отчетности должен сообщать Работодателю об изменении своих персональных данных. Для этого Работник обязан в течение 5 (пяти) рабочих дней с даты получения документа, подтверждающего изменения, представить делопроизводителю:

- при изменении имени, фамилии, отчества – паспорт, свидетельство о смене имени, фамилии или отчества;
- при смене местожительства (прописки) – паспорт с отметкой о новом местожительстве;
- при вступлении в брак – свидетельство о вступлении в брак, паспорт с новой фамилией (в случае смены фамилии);
- при расторжении брака – свидетельство о расторжении брака, паспорт с новой фамилией (в случае смены фамилии);
- при рождении ребенка – свидетельство о рождении ребенка;
- при получении образования, повышении квалификации: диплом, удостоверение, свидетельство и др.;
- при получении награды, звания — приказ, распоряжение, наградной лист или свидетельство о награждении и др.;

- при изменении сведений воинского учета – военный билет и другие документы об изменении сведений, необходимых для ведения воинского учета.

2.6. По мере необходимости работодатель истребует у сотрудника дополнительные сведения. Сотрудник предоставляет требуемые сведения и в случае необходимости предъявляет документы, подтверждающие достоверность этих сведений.

2.6. Чтобы обрабатывать персональные данные сотрудников, работодатель получает от каждого сотрудника согласие на обработку его персональных данных. Такое согласие работодатель получает, если закон не предоставляет работодателю права обрабатывать персональные данные без согласия сотрудников.

2.7. Согласие на обработку персональных данных может быть отозвано работником. В случае отзыва работником согласия на обработку персональных данных работодатель вправе продолжить обработку персональных данных без согласия работника при наличии оснований, указанных в пунктах 2–11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ.

3. Хранение и обработка персональных данных сотрудников с использованием средств автоматизации

3.1. МКУ «Административно-хозяйственная служба» обеспечивает защиту персональных данных работников от неправомерного использования или утраты.

3.2. Личные дела (личные карточки при наличии) хранятся в бумажном виде в папках, прошитые и пронумерованные по страницам. Личные дела (личные карточки при наличии) находятся у делопроизводителя в специально отведенном шкафу, обеспечивающем защиту от несанкционированного доступа.

3.3. Персональные данные сотрудников могут также храниться в электронном виде в локальной компьютерной сети. Доступ к электронным базам данных, содержащим персональные данные сотрудников, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли устанавливаются руководителем организации и сообщаются индивидуально сотрудникам, имеющим доступ к персональным данным сотрудников.

3.4. Изменение паролей руководителем организации происходит не реже одного раза в два месяца.

3.5. Доступ к персональным данным сотрудника имеют руководитель организации, его заместитель, главный бухгалтер, а также непосредственный руководитель
сотрудника. Специалисты отдела бухгалтерии, делопроизводитель – к тем данным, которые необходимы для выполнения конкретных функций. Доступ специалистов других отделов к персональным данным осуществляется на основании письменного разрешения руководителя организации или его заместителя.

3.6. Копировать и делать выписки из персональных данных сотрудника разрешается исключительно в служебных целях с письменного разрешения руководителя организации, его заместителя и главного бухгалтера.

4. Использование персональных данных сотрудников

4.1. Персональные данные сотрудника используются для целей, связанных с выполнением сотрудником трудовых функций.

4.2. Работодатель использует персональные данные, в частности, для решения вопросов продвижения сотрудника по службе, очередности предоставления ежегодного отпуска, установления размера зарплаты. На основании персональных данных сотрудника решается вопрос о допуске его к информации, составляющей служебную или коммерческую тайну.

4.3. При принятии решений, затрагивающих интересы сотрудника, работодатель не имеет права основываться на персональных данных сотрудника, полученных исключительно в результате их автоматизированной обработки или электронного поступления. Работодатель также не вправе принимать решения, затрагивающие интересы сотрудника, основываясь на данных, допускающих двоякое толкование. В случае если на основании персональных данных сотрудника невозможно достоверно установить какой-либо факт, работодатель предлагает сотруднику представить письменные разъяснения.

5. Передача персональных данных сотрудников

5.1. Информация, относящаяся к персональным данным сотрудника, может быть предоставлена государственным органам в порядке, установленном федеральным законом.

5.2. Работодатель не вправе предоставлять персональные данные сотрудника третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника, а также в случаях, установленных федеральным законом.

5.3. В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом или настоящим Положением на получение информации, относящейся к персональным данным сотрудника, работодатель обязан отказать лицу в выдаче информации. Лицу, обратившемуся с запросом, выдается уведомление об отказе в выдаче информации, копия уведомления подшивается в личное дело сотрудника.

5.4. Персональные данные сотрудника могут быть переданы представителям сотрудников в порядке, установленном Трудовым кодексом РФ, в том объеме, в каком это необходимо для выполнения указанными представителями их функций.

5.5. Передача (распространение, предоставление, доступ) персональных данных, разрешенных работником для распространения, должна быть прекращена в любое время по его требованию.

6. Гарантии конфиденциальности персональных данных сотрудников

6.1. Информация, относящаяся к персональным данным сотрудника, является служебной тайной и охраняется законом.

6.2. Сотрудник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

6.3. В случае разглашения персональных данных сотрудника без его согласия он вправе требовать от работодателя разъяснений и обжаловать в суде любые неправомерные действия или бездействие работодателя при обработке и защите персональных данных сотрудника.

Приложение № 2

УТВЕРЖДАЮ
И. о. директора МКУ
«Административно-хозяйственная служба»
_____ А.А. Кузнецов
«26» 05 2025 г.

ПОЛОЖЕНИЕ
о защите персональных данных

1. Общие положения

1.1. Положение о защите персональных данных МКУ «Административно-хозяйственная служба» (далее – организация, Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.

1.2. Цель настоящего Положения – защита персональных данных клиентов, контрагентов и пользователей сайта https://мку-ахс.рф МКУ «Административно-хозяйственная служба» от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

1.3. В целях настоящего Положения:

- под персональными данными (далее – ПД) понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных;
- под угрозами безопасности ПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- под уровнем защищенности ПД понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает

нейтрализацию определенных угроз безопасности ПД при их обработке в информационной системе.

1.4. Настоящее Положение и изменения к нему утверждаются директором МКУ «Административно-хозяйственная служба» и вводятся приказом. Настоящее Положение размещается на официальном сайте МКУ «Административно-хозяйственная служба» по адресу https://мку-ахс.рф в свободном доступе.

1.5. Настоящее Положение вступает в силу с 26.05.2025.

2. Защита персональных данных

2.1. Организация принимает следующие меры по защите ПД:

2.1.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением организацией требований к защите ПД.

2.1.2. Разработка политики в отношении обработки ПД.

2.1.3. Установление правил доступа к ПД, обеспечение регистрации и учета всех действий, совершаемых с ПД.

2.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.

2.1.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.

2.1.7. Соблюдение условий, обеспечивающих сохранность ПД и исключающих
несанкционированный доступ к ним.

2.1.8. Обнаружение фактов несанкционированного доступа к ПД.

2.1.9. Восстановление ПД, модифицированных или уничтоженных вследствие
несанкционированного доступа к ним.

2.1.10. Изучение работниками, непосредственно осуществляющими обработку ПД, положений законодательства РФ о персональных данных, в том

биометрические ПД, или при третьем типе угрозы организация обрабатывает общие ПД более чем 100 тыс. физических лиц.

2.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы организация обрабатывает только общие ПД субъектов персональных данных или менее чем 100 тыс. физических лиц.

2.4. При четвертом уровне защищенности персональных данных организация:

- обеспечивает режим безопасности помещений, в которых размещается информационная система;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до ПД субъектов персональных данных;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, организация назначает ответственного за обеспечение безопасности ПД в информационной системе.

2.6. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4, 2.5 настоящего Положения, организация ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.

2.7. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4—2.6 настоящего Положения, организация:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе;
- создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов.

2.8. В целях защиты ПД на бумажных носителях организация:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД субъектов персональных данных;
- хранит документы, содержащие ПД субъектов персональных данных в шкафах, запирающихся на ключ.

числе требований к защите персональных данных, документов, определяющих политику организации в отношении обработки ПД, локальных актов по вопросам обработки персональных данных.

2.1.11. Осуществление внутреннего контроля и аудита.

2.1.12. Определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.

2.2. Угрозы защищенности персональных данных:

2.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.

2.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.

2.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.

2.3. Уровни защищенности персональных данных:

2.3.1. Первый уровень защищенности. Если организация отнесла информационную систему к первому типу угрозы или если тип угрозы второй, но организация обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета работников.

2.3.2. Второй уровень защищенности. Если тип угрозы второй и организация обрабатывает специальные категории ПД субъектов персональных данных, вне зависимости от их количества, или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы организация обрабатывает специальные категории данных более чем 100 тыс. физических лиц.

2.3.3. Третий уровень защищенности. Если при втором типе угрозы организация обрабатывает общие ПД субъектов персональных данных или менее чем 100 тыс. физических лиц, или при третьем типе угрозы организация обрабатывает специальные категории ПД субъектов или менее чем 100 тыс. физических лиц, или при третьем типе угрозы организация обрабатывает

2.9. В целях обеспечения конфиденциальности документы, содержащие ПД субъектов персональных данных, оформляются, ведутся и хранятся только работниками бухгалтерии и делопроизводителем.

2.10. Работники бухгалтерии и делопроизводитель, допущенные к ПД работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД не допускаются.

2.11. Передача ПД по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия субъекта персональных данных на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.

2.12. Передача информации, содержащей сведения о ПД субъекта персональных данных, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.

3. Гарантии конфиденциальности персональных данных

3.1. Все работники организации, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства РФ.

3.2. Субъект персональных данных вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.

3.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.

Приложение № 3

УТВЕРЖДАЮ
И. о. директора МКУ
«Административно-хозяйственная служба»
_____ А.А. Кузнецов
«26» 05 2025 г.

ПОЛОЖЕНИЕ

О порядке уничтожения персональных данных

1. Общие положения

1.1. Настоящее Положение о порядке уничтожения персональных данных в МКУ «Административно-хозяйственная служба» (далее – Положение) устанавливает периодичность и способы уничтожения носителей, содержащих персональные данные субъектов персональных данных.

1.2. Целью настоящего Положения является обеспечение защиты прав и свобод работников при обработке их персональных данных в МКУ «Административно-хозяйственная служба» (далее – организация).

1.3. Основные понятия, используемые в Положении:

- субъект персональных данных – работник и (или) иное лицо, к которому относятся соответствующие персональные данные;
- работник – физическое лицо, вступившее в трудовые отношения с организацией;
- персональные данные – информация, сохраненная в любом формате, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), которая сама по себе или в сочетании с другой информацией, имеющейся в организации, позволяет идентифицировать личность субъекта персональных данных;

- обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;
- уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;
- носители персональных данных – как электронные (компакт-диски, флеш- накопители и др.), так и неэлектронные (бумажные) носители персональных данных.

1.4. Настоящее Положение разработано на основе Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и других нормативных правовых актов.

2. Правила уничтожения носителей, содержащих персональные данные

2.1. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, должно соответствовать следующим правилам:

- быть конфиденциальным, исключая возможность последующего восстановления;
- оформляться юридически, в частности, актом об уничтожении персональных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных организации;
- уничтожение должно касаться только тех носителей, содержащих персональные данные субъектов персональных данных, которые подлежат уничтожению в связи с истечением срока хранения, достижением цели обработки указанных персональных данных либо утратой необходимости в их достижении, не допуская случайного или преднамеренного уничтожения актуальных носителей.

3. Порядок уничтожения носителей, содержащих персональные данные

3.1. Персональные данные субъектов персональных данных хранятся не дольше, чем этого требуют цели их обработки, и подлежат уничтожению по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении.

3.2. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются в специально отведенном для этих целей помещении

комиссией по уничтожению персональных данных, утвержденной приказом директора организации (далее – Комиссия).

3.3. Носители, содержащие персональные данные субъектов персональных данных, уничтожаются Комиссией в срок, не превышающий 30 дней с даты достижения целей обработки персональных данных либо утраты необходимости в их достижении, а также в случае, если истек срок их хранения.

3.4. Комиссия производит отбор бумажных носителей персональных данных, подлежащих уничтожению, с указанием оснований для уничтожения.

3.5. На все отобранные к уничтожению документы составляется акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.6. В актах о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению исправления не допускаются.

3.7. Комиссия проверяет наличие всех документов, включенных в акт о выделении носителей, содержащих персональные данные субъектов персональных данных, к уничтожению.

3.8. По окончании сверки акт о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению подписывается всеми членами Комиссии и утверждается проректором по направлению.

3.9. Носители, содержащие персональные данные субъектов персональных данных, отобранные для уничтожения и включенные в акт, после проверки их Комиссией передаются ответственному за уничтожение документов в помещение делопроизводителя.

3.10. Уничтожение носителей, содержащих персональные данные субъектов персональных данных, производится после утверждения акта в присутствии всех членов Комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте носителей.

3.11. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

3.12. Уничтожение носителей, содержащих персональные данные, осуществляется в следующем порядке:

- уничтожение персональных данных, содержащихся на бумажных носителях, осуществляется путем измельчения на мелкие части, исключающие возможность последующего восстановления информации. Измельчение осуществляется с использованием шредера (уничтожителя документов), установленного в помещении делопроизводителя, либо документы передаются на переработку (утилизацию) организациям, собирающим вторсырье (пункты приема макулатуры);
- уничтожение персональных данных, содержащихся на машиночитаемых носителях, осуществляется путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления данных. Вышеуказанное достигается путем деформирования, нарушения единой целостности носителя;
- подлежащие уничтожению файлы с персональными данными субъектов персональных данных, расположенные на жестком диске, удаляются средствами операционной системы компьютера с последующим «очищением корзины»;
- в случае допустимости повторного использования носителя CD-RW, DVD-RW применяется программное удаление («затирание») содержимого диска путем его форматирования с последующей записью новой информации на данный носитель.

4. Порядок сдачи макулатуры

4.1. Документы по истечении срока хранения, достижении целей обработки или в случае утраты необходимости в их достижении подлежат уничтожению путем сдачи организациям, собирающим вторсырье (пункты приема макулатуры).

4.2. Выделенные документы по акту о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению передаются к уничтожению в упакованном виде.

4.3. Документы, подлежащие вывозу, не должны содержать бумагу и картон, не пригодные для переработки; бумагу и картон, покрытые полиэтиленом и другими полимерными пленками; материал, выделяющий ядовитые и токсичные вещества.

4.4. Документы, подлежащие вывозу, не должны содержать:

- тряпье, веревку, шпагат из лубяных волокон и полимеров;
- металлические и деревянные изделия, кусочки стекла и керамики, камень, уголь, слюду, целлофан, целлулоид, полимерные материалы в виде изделий (пленок, гранул), пенопласт, искусственную и натуральную кожу, клеенку, битум, парафин, остатки химических и минеральных веществ и красок;
- влажность документов, подлежащая вывозу, должна быть не более 10 процентов.

4.5. Сдача оформляется приемо-сдаточными накладными, данные которых (дата сдачи, номер накладной, вес сданной макулатуры) указываются в акте о выделении документов, содержащих персональные данные субъектов персональных данных, к уничтожению.

4.6. Погрузка и вывоз документов осуществляются под контролем лица, ответственного за обеспечение сохранности документов.

4.7. Отобранные к уничтожению документы перед сдачей на переработку в качестве макулатуры должны в обязательном порядке измельчаться до степени, исключающей возможность прочтения текста.

5. Порядок оформления документов об уничтожении персональных данных

5.1. Если обработка персональных данных осуществлялась без использования средств автоматизации, об уничтожении носителей, содержащих персональные данные, Комиссия составляет и подписывает акт об уничтожении персональных данных.

5.2. Если обработка персональных данных осуществлялась с использованием средств автоматизации, об уничтожении носителей, содержащих персональные данные, Комиссия составляет и подписывает акт об уничтожении персональных данных, а также осуществляет выгрузку из журнала регистрации событий в информационной системе персональных данных организации.

5.3. Если обработка персональных данных осуществлялась одновременно с использованием средств автоматизации и без использования средств автоматизации, об уничтожении носителей, содержащих персональные данные, Комиссия составляет и подписывает акт об уничтожении персональных данных, а также осуществляет выгрузку из журнала регистрации событий в информационной системе персональных данных организации.

5.4. Акт об уничтожении персональных данных составляется по установленной форме. Акт об уничтожении персональных данных может быть составлен как в бумажной, так и электронной форме.

В акте указываются:

- наименование и адрес организации;
- наименование организации, которая осуществляла обработку персональных данных по поручения организации;
- Ф. И. О. сотрудников, чьи персональные данные были уничтожены;
- Ф. И. О. и должности сотрудников, уничтоживших персональные данные, а также их подписи;
- перечень категорий уничтоженных персональных данных;
- наименование уничтоженных носителей, содержащих персональные данные, с указанием количества листов в отношении каждого материального носителя – в случае обработки персональных данных без использования средств автоматизации;
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные – в случае обработки персональных данных с использованием средств автоматизации;
- способ уничтожения персональных данных;
- причина уничтожения персональных данных;
- дата уничтожения персональных данных.

5.5. Выгрузка из журнала регистрации событий в информационной системе персональных данных организации содержит:

- Ф. И. О. сотрудников, чьи персональные данные были уничтожены;
- перечень категорий уничтоженных персональных данных;
- наименование информационной системы персональных данных, из которой были уничтожены персональные данные;
- причину уничтожения персональных данных;
- дату уничтожения персональных данных.

5.6. Факт уничтожения носителей, содержащих персональные данные субъектов персональных данных, фиксируется в журнале учета документов, переданных на уничтожение. Данный документ является документом конфиденциального характера и вместе с актом об уничтожении персональных данных и выгрузкой из журнала хранится в помещении делопроизводителя в течение трех лет. По истечении срока хранения акт об уничтожении персональных данных и выгрузка из журнала, передаются в архив организации на хранение.

6. Ответственность руководителей структурных подразделений

6.1. Ответственным лицом за организацию хранения документов является делопроизводитель.

6.2. Делопроизводитель может быть привлечен к административной ответственности за нарушение требований по организации хранения документов, содержащих персональные данные.

Приложение № 4

УТВЕРЖДАЮ
И. о. директора МКУ
«Административно-хозяйственная служба»
_____ А.А. Кузнецов
«26» 05 2025 г.

ПОЛОЖЕНИЕ
о внутреннем контроле работы с персональными данными
МКУ «Административно-хозяйственная служба»

1. Настоящее положение о внутреннем контроле соответствия работы с персональными данными требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами МКУ «Административно-хозяйственная служба» (далее – Положение), устанавливает порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МКУ «Административно-хозяйственная служба» (далее – организация).

2. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных в обществе осуществляется в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящем Положении, применяются в том же значении, что и в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных».

4. Целью настоящего Положения является обеспечение защиты персональных данных сотрудников общества от несанкционированного доступа, неправомерного их использования или утраты, определение порядка и правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

5. Настоящее Положение устанавливает и определяет:

- виды и периодичность внутреннего контроля;
- порядок создания комиссии для осуществления внутреннего контроля;
- порядок проведения внутренней проверки.

6. Внутренний контроль соответствия обработки персональных данных делится на текущий и комиссионный.

7. Текущий внутренний контроль осуществляется на постоянной основе ответственным за организацию обработки персональных данных в организации, руководителями направлений деятельности и структурных подразделений организации и операторами информационных систем персональных данных в ходе мероприятий по обработке персональных данных.

Ответственный за организацию обработки персональных данных в организации имеет право:

- запрашивать у сотрудников организации информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства РФ;
- вносить руководителю организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства РФ в отношении обработки персональных данных.

8. Комиссионный внутренний контроль осуществляется комиссией, образуемой приказом руководителя организации из числа сотрудников

организации, допущенных к обработке персональных данных. Периодичность проверки – не реже одного раза в год.

Комиссионные проверки соответствия обработки персональных данных установленным требованиям в организации проводятся на основании утвержденного руководителем плана осуществления комиссионного внутреннего контроля соответствия обработки персональных данных установленным требованиям, разрабатываемого председателем комиссии, или на основании поступившего письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки).

Внеплановые проверки организуются в течение трех рабочих дней с момента поступления соответствующего заявления.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в ее результатах.

9. При проведении внутренней проверки соответствия обработки персональных данных установленным требованиям комиссией должно быть полностью, объективно и всесторонне установлено соответствие по следующим положениям:

- наличие, учет, порядок хранения и обезличивания персональных данных;
- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

10. В отношении персональных данных, ставших известными членам комиссии или ответственному за организацию обработки персональных данных в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

11. Срок проведения проверки комиссией не может составлять более 20 дней со дня принятия решения о ее проведении.

12. Результаты проверки оформляются в виде протокола проведения внутренней проверки.

13. При выявлении в ходе проверки нарушений ответственным за организацию обработки персональных данных в организации либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

14. Протоколы хранятся у ответственного за организацию обработки персональных данных в течение текущего года. Уничтожение протоколов проводится ответственным за организацию обработки персональных данных самостоятельно в январе года, следующего за проверочным годом.

15. О результатах проверки и мерах, необходимых для устранения нарушений, руководителю общества докладывает ответственный за организацию обработки персональных данных в организации либо председатель комиссии.

Приложение № 5

УТВЕРЖДАЮ
И. о. директора МКУ
«Административно-хозяйственная служба»
_____ А.А. Кузнецов
«20» 05 2025 г.

Регламент
о допуске работников к обработке персональных данных третьих лиц

1. Общие положения

1.1. Регламент допуска работников к обработке персональных данных клиентов, контрагентов и третьих лиц, сотрудничающих с МКУ «Административно-хозяйственная служба», разработан в соответствии с Трудовым кодексом, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и иными нормативно-правовыми актами.

1.2. Настоящий Регламент определяет порядок допуска работников к обработке персональных данных клиентов, контрагентов и третьих лиц, и гарантии конфиденциальности сведений о клиентах, контрагентах и третьих лицах, которые они предоставили МКУ «Административно-хозяйственная служба.

1.3. Настоящий Регламент вступает в силу с 26.05.2025.

2. Виды допуска к обработке персональных клиентов, контрагентов и третьих лиц

2.1. Допуск работников к обработке персональных данных клиентов, контрагентов и третьих лиц подразделяется на полный и частичный.

2.2. Полный допуск к обработке персональных данных клиентов, контрагентов и третьих лиц имеют директор организации, его заместитель, главный бухгалтер.

2.3. Частичный допуск к обработке персональных данных клиентов, контрагентов и третьих лиц имеют:

- работники бухгалтерии — к обработке тех данных, которые необходимы для выполнения их непосредственных должностных обязанностей;
- делопроизводитель — к обработке тех данных, которые необходимы для выполнения их непосредственных должностных обязанностей.

2.4. Лицам, не указанным в пункте 2.3 настоящего Регламента, частичный допуск к обработке персональных данных клиентов, контрагентов и третьих лиц может быть предоставлен на основании письменного разрешения руководителя организации или его заместителя.

3. Порядок допуска работников к обработке персональных данных

3.1. Лица, указанные в пунктах 2.2, 2.3 настоящего Регламента, допускаются к обработке персональных данных клиентов, контрагентов и третьих лиц с соблюдением общей процедуры оформления работы с персональными данными, предусмотренной действующим законодательством и локальными актами МКУ «Административно-хозяйственная служба», без дополнительного оформления.

3.2. Лица, указанные в пункте 2.4 настоящего Регламента, заинтересованные в частичном допуске к обработке персональных данных клиентов, контрагентов и третьих лиц, направляют директору, его заместителю мотивированное ходатайство, в котором излагают:

- цель допуска к обработке персональных данных клиентов, контрагентов и третьих лиц;
- перечень персональных данных, допуск к обработке которых необходим;
- обоснование необходимости и целесообразности допуска к обработке персональных данных клиентов, контрагентов и третьих лиц.

3.3. Ходатайство подлежит рассмотрению в течение трех рабочих дней. По результатам рассмотрения ходатайства руководитель организации или его заместитель издает распоряжение о допуске работника к обработке персональных данных других работников либо принимает решение об отказе в допуске с указанием причин отказа.

4. Порядок прекращения допуска работников к обработке персональных данных

4.1. Допуск к обработке персональных данных клиентов, контрагентов и третьих лиц прекращается:

- при увольнении работника, имеющего допуск;
- при переводе работника, имеющего допуск, на должность, выполнение работ по которой уже не требует допуска к обработке персональных данных клиентов, контрагентов и третьих лиц.

4.2. Допуск к обработке персональных данных у лиц, указанных в пункте 2.4 настоящего Регламента, может быть дополнительно прекращен по письменному решению директора или его заместителя.