Утверждаю

Директор МУП «ЖКХ Ирбитского района»

_____М.А. Сивков

«09» января 2024г.

ПОЛОЖЕНИЕ
о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МУП «ЖКХ ИРБИТСКОГО РАЙОНА» Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам РФ

1. Общие положения:

1.1 Настоящее Положение о внутреннем контроле и (или) аудите определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных в **МУП «ЖКХ ИРБИТСКОГО РАЙОНА»** (далее Организация) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

1.2 Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации 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 с использованием средств автоматизации и без использования таковых средств» и принятыми в соответствии с ними нормативными правовыми актами.

1.3. Исполнение Положения обязательно для всех работников Организации, осуществляющих обработку персональных данных, как без использования средств автоматизации, так и в информационных системах обработки персональных данных.

1.4. В настоящем Положении используются основные понятия в значениях, определенных статьей 3 от 27.07.2006 № 152-ФЗ «О персональных данных».

1.5. Внутренний контроль соответствия обработки персональных данных – контроль соответствия обработки персональных данных в Организации требованиям законодательства в сфере обработки персональных данных, проводимый силами Организации в соответствии с Положением и другими локальными нормативными актами Организации.

1.6. Внутренний аудит соответствия обработки персональных данных – контроль соответствия обработки персональных данных в Организации требованиям законодательства в сфере обработки персональных данных, проводимый специализированными организациями, привлекаемыми Организацией по договорам оказания услуг в соответствии с локальными нормативными актами Организации.

2. Порядок проведения внутреннего контроля:

2.1. Внутренний контроль соответствия обработки персональных данных осуществляется комиссией по плану мероприятий внутреннего контроля, утверждаемому ежегодно Директором Организации.

2.2. Мероприятия внутреннего контроля могут быть внеплановыми по решению комиссии, если есть фактические основания полагать, что процедура обработки персональных данных в Организации не соответствует требованиям законодательства

Российской Федерации. Проведение внеплановой проверки организуется председателем комиссии, а в его отсутствие — заместителем председателя комиссии в течение трех рабочих дней с даты поступления письменного заявления работника о нарушении правил обработки персональных данных.

2.3. Состав комиссии утверждается Директором Организации.

2.4. Проверки по предметам контроля, указанным в акте, согласно Приложения, к настоящему Положению, могут осуществляться как непосредственно на рабочих местах исполнителей, участвующих в обработке персональных данных, так и путем направления запросов и рассмотрения документов, необходимых для осуществления внутреннего контроля.

2.5. При проведении мероприятия внутреннего контроля должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- 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 и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

2.6. Проверки соответствия обработки персональных данных, установленных требованиям в Организации, проводятся один раз в год, план проведения внутреннего контроля на очередной год формируется директором Организации до 15 декабря, утвержденный план очередности проведения внутреннего контроля доводится до работников Организации.

2.7. Комиссия при проверке внутреннего контроля имеет право:

- запрашивать у работников, осуществляющих обработку персональных данных информацию и документы, необходимые для осуществления внутреннего контроля;
- требовать от ответственных 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 Российской Федерации;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке в Организации;
- вносить предложения о привлечении к дисциплинарной ответственности работников, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.8. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

2.9. Мероприятие внутреннего контроля не может длиться больше 10 рабочих дней. Срок мероприятия может быть продлен распорядительным актом Директора Организации при наличии оснований, не позволяющих закончить контрольное мероприятие не позднее чем через 10 дней с даты начала проверки.

3. Оформление результатов внутреннего контроля.

3.1. Результаты проведенной проверки внутреннего контроля соответствия обработки персональных данных оформляются комиссией в виде акта внутреннего контроля, составленного по форме согласно Приложения настоящего Положения, который подписывается всеми членами комиссии, и утверждается председателем комиссии, а в его отсутствие — заместителем председателя комиссии, если предусматривает план мероприятий внутреннего контроля или распорядительный акт Директора Организации члены комиссии обязаны составлять докладные записки по итогам контрольных мероприятий.

3.2. Выявленные в ходе внутреннего контроля нарушения фиксируются в акте внутреннего контроля с предложениями мероприятий по устранению нарушений и сроков их выполнения.

3.3. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости комиссия докладывает на очередном совещании Директору Организации, если иное не установлено локальными актами Организации.

3.4. Акты внутреннего контроля, докладные записки по итогам контрольных мероприятий хранятся в запирающемся шкафу в юридическом отделе (кабинет №1) Организации.

4. Порядок проведения внутреннего аудита.

4.1. Внутренний аудит соответствия обработки персональных данных проводится в случаях, когда Организация не может объективно оценить соответствие обработки персональных данных в Организации требованиям законодательства в сфере обработки персональных данных.

4.2. Внутренний аудит организуется на основании распорядительного акта Директора Организации.

4.3. Внутренний аудит проводит организация, которая в соответствии со своими учредительными документами занимается оценкой рисков в обработке персональных данных и возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.4. На время проведения внутреннего аудита Директор Организации назначает ответственного, который должен взаимодействовать с организацией, проводящей аудит (далее – аудитор).

4.5. Ответственный обязан:

- обеспечить аудитора всей необходимой информацией;
- организовать условия для работы;
- оказывать помощь при возникновении трудностей;
- контролировать работу аудитора;
- принимать все отчеты аудитора и доводить их до сведения Директору Организации.

4.6. Действия и обязанности аудитора определяются заключенным договором оказания услуг по проведению внутреннего аудита.

4.7. Документы внутреннего аудита, в том числе итоговые отчеты, хранятся в запирающемся шкафу в кабинете Директора организации.

УТВЕРЖДАЮ
Директор
МУП «ЖКХ Ирбитского района»
Сивков М.А.
9 января 2024 г.

АКТ

внутреннего контроля (аудита) соответствия обработки персональных данных в МУП ЖКХ «Ирбитского района» требованиям к защите персональных данных

1. Результаты рассмотрения вопросов по предметам аудита:

Предмет аудита	Результат рассмотрения	Примечание
Документы, определяющие основания обработки персональных данных	Соответствуют требованиям законодательства	
Утвержденный перечень работников МУП ЖКХ «Ирбитского района», доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими трудовых обязанностей	Перечень утвержден, соответствует требованиям законодательства	
Утвержденные перечни информационных систем персональных данных, эксплуатируемых в МУП ЖКХ «Ирбитского района»	Перечень утвержден, соответствует требованиям законодательства	
Своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в МУП ЖКХ «Ирбитского района», в связи с достижением целей обработки или	Мероприятия проводятся	

утраты необходимости в достижении этих целей		
Отсутствие неправомерно размещенных персональных данных граждан на официальном сайте МУП ЖКХ «Ирбитского района»	Неправомерно размещенных данных нет	
…		