

_____/ Горошко С.А.

Положение
об аудите при обработке персональных данных

1. Общие положения

1.1. Настоящее Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в ООО «Самария Трейд» требованиям законодательства в сфере обработки персональных данных (далее - Положение) разработано в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных в ООО «Самария Трейд» (далее - организация) требованиям к защите персональных данных, установленным законодательством Российской Федерации.

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 Положении используются основные понятия в значениях, определённых статье 3 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

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.

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 Руководителем 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.

2.3. Состав комиссии утверждается Директором организации.

2.4. Мероприятия внутреннего контроля могут осуществляться как непосредственно на рабочих местах исполнителей, участвующих в обработке персональных данных, так и путём 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 учёта 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. Комиссия при проведении внутреннего контроля имеет право:

- запрашивать у работников, осуществляющих обработку персональных данных, информацию и (или) документы, необходимые для осуществления внутреннего контроля;
- требовать у ответственных за обработку персональных данных уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путём 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.

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

2.8. Мероприятие внутреннего контроля не может длиться больше 10 рабочих дней. Срок мероприятия может быть продлён распорядительным актом Руководителя организации при наличии оснований, не позволяющих закончить контрольное мероприятие за 10 рабочих дней.

3. Оформление итогов внутреннего контроля

3.1. Результаты внутреннего контроля соответствия обработки персональных данных оформляются комиссией в виде акта внутреннего контроля, составленного по форме согласно Приложению к Положению. Члены комиссии обязаны составлять докладные записки по итогам контрольных мероприятий, если это предусматривает план мероприятий внутреннего контроля или распорядительный акт Директора организации.

3.2. Акт внутреннего контроля подписывается всеми членами комиссии.

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

3.4. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости комиссия докладывает на очередном совещании при Директоре организации, если иное не установлено локальными актами организации.

3.5. Акты внутреннего контроля, докладные записки по итогам контрольных мероприятий хранятся запирающемся шкафу в кабинете Директора 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 г. № 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 отчёты аудитора и доводить их до сведения Директора организации. Действия и обязанности аудитора определяются заключённым договором оказания услуг по проведению внутреннего аудита. Документы внутреннего аудита, в том числе итоговые отчёты, хранятся в запирающемся шкафу в кабинете Директора организации.

ОБРАЗЕЦ

АКТ

Внутреннего контроля соответствия обработки персональных данных в ООО «Самария Трейд» требованиям законодательства в сфере обработки персональных данных

«___» _____ 202__ г.

№ 1

Комиссия ООО «Самария Трейд» в составе:

- председателя:

- членов комиссии:

провела внутренний контроль соответствия обработки персональных данных в ООО «Самария Трейд» требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на 202__ год, утверждённым приказом Директора ООО «Самария Трейд» от «___» _____ 202__ г. № ____.

В ходе контрольных мероприятий проверены:

- документы, определяющие основания обработки персональных данных;
- утверждённый перечень работников № _____, имеющих доступ к персональным данным в силу своих служебных обязанностей;
- своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в ООО «Самария Трейд», в связи с достижением целей обработки или утраты необходимости в достижении этих целей;
- отсутствие неправомерно размещенных персональных данных на сайте ООО «Самария Трейд» и иных общедоступных местах;
- анализ содержания сайта ООО «Самария Трейд».

Выявленные нарушения:

- Срок устранения нарушений:

Ответственный за исполнение:

Подписи членов комиссии:

**План-график мероприятий внутреннего контроля
соответствия обработки персональных данных на 2025 год**

Мероприятие	Ответственный	Срок исполнения
Проверка соблюдения правил доступа к персональным данным	еженедельно	Ответственный за обеспечение безопасности персональных данных
Проверка соблюдения режима защиты	ежедневно	Ответственный за обеспечение безопасности персональных данных
Проверка выполнения антивирусной политики	еженедельно	Ответственный за обеспечение безопасности персональных данных
Проверка обновления ПО и единообразия применяемого ПО на всех устройствах, используемых при обработке персональных данных	еженедельно	Ответственный за обеспечение безопасности персональных данных
Проверка актуальности локальных нормативных актов в сфере обработки персональных данных	ежегодно	Ответственный за обеспечение безопасности персональных данных
Рассмотрение итогов мероприятий внутреннего контроля на совещании при директоре	ежегодно	Ответственный за обеспечение безопасности персональных данных