

УТВЕРЖДАЮ
Заведующий отделом социальной
защиты населения Администрации
Матвеево-Курганского района



Г.А. Колесникова

2017 г.

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Отделе социальной защиты населения Администрации Матвеево-Курганского района

1. Общие положения

Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в Отделе социальной защиты населения Администрации Матвеево-Курганского района (далее – Учреждение) определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных; основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

Настоящие Правила разработаны в соответствии Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации» и другими нормативными правовыми актами.

В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

2. Правила осуществления внутреннего контроля

1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организовывается проведение периодических проверок условий обработки персональных данных.

2. Проверки осуществляются ответственным за организацию обработки персональных данных в Учреждении.

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

3. Проверки соответствия обработки персональных данных установленным требованиям в Учреждении проводятся на основании утвержденного ежегодного плана (приложение) осуществления внутреннего контроля соответствия обработки

конфиденциальной информации установленным требованиям или на основании поступившего в Учреждение письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.

4. При проведении проверки соответствия обработки персональных данных установленным требованиям 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 до ввода в эксплуатацию информационной системы 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.

5. Ответственный за организацию обработки персональных данных в Учреждении имеет право:

- запрашивать у сотрудников Учреждения информацию, необходимую для реализации полномочий;
- требовать от уполномоченных на обработку персональных данных сотрудников 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;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

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

7. Проверка должна быть завершена не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, начальнику докладывает ответственный за организацию обработки персональных данных, в форме письменного заключения.

8. Начальник, назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.

Приложение
к правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям к
защите персональных данных

Форма плана внутренней проверки состояния защиты конфиденциальной
информации

Мероприятие	Период проверки	Исполнитель
1. Проверка полноты и качества разработанных распорядительных и нормативно-методических документов, регламентирующих обеспечение безопасности конфиденциальной информации (персональных данных)		
2. Контроль выполнения требований по режиму доступа в защищаемые помещения и на автоматизированные рабочие места, обрабатывающие конфиденциальной информации (персональных данных)		
3. Проверка порядка использования технических средств защиты конфиденциальной информации		
4. Проверка выполнения требований распорядительных и нормативно-методических документов, регламентирующих обеспечение безопасности конфиденциальной информации (персональных данных)		
5. Подведение итогов		
6. Составление акта проверки		
7. Доклад председателю по результатам проверки		