

Муниципальное общеобразовательное учреждение
«Средняя школа № 1 с углубленным изучением отдельных предметов г. Котово»
Котовского муниципального района Волгоградской области»
(МБОУ СШ № 1 г. Котово)
403805 обл. Волгоградская, г. Котово, ул. Школьная, 3 тел.факс 4-39-13, 4-40-59,
ОКПО 41477010, ОГРН 1023404974768, ИНН 3414012422 КПП 341401001
e-mail: KotovoSchool@yandex.ru



УТВЕРЖДАЮ:

Директор школы *М. А. Дронина*
г. Котово
приказ № 335 от 27.12.2018

**Правила осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных
в МБОУ СШ № 1 г. Котово**

1. Настоящими Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в МБОУ СШ № 1 г. Котово (далее – Организации) 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.
2. 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», Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» и другими нормативными правовыми актами.
3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. № 152 ФЗ «О персональных данных».
4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Организации организовывается проведение периодических проверок условий обработки персональных данных.
5. Проверки осуществляются ответственным за организацию обработки персональных данных в Организации либо комиссией, образуемой приказом руководителя организации.

В проведении проверки не может участвовать гражданский служащий, прямо или косвенно заинтересованный в её результатах.

6. Проверки соответствия обработки персональных данных установленным требованиям в Организации проводятся на основании утвержденного начальником Управления Роскомнадзора ежегодного плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям или на основании поступившего в Управление Роскомнадзора письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления.
7. 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.
8. Ответственный за организацию обработки персональных данных в Организации (комиссия) 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 Российской Федерации;
 - вносить руководителю организации предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
 - вносить руководителю организации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.
9. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных в Организации в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

10. 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, руководителю организации докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.
11. Руководитель организации, назначивший внеплановую проверку, обязан контролировать своевременность и правильность её проведения.