

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
«СРЕДНЯЯ ШКОЛА № 6» г. Кольчугино  
(МБОУ «Средняя школа №6»)**

ПРИНЯТО

Общим собранием работников  
МБОУ «Средняя школа №6»  
(протокол от 28.12.2022 г. №3)

**УТВЕРЖДАЮ**  
Директор МБОУ «Средняя школа №6»  
С.В. Старостина  
Приказ №1 от 09 января 2023 г.



**Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МБОУ «Средняя школа №6» требованиям законодательства в сфере обработки персональных данных**

**1. Общие положения**

1.1. Настоящее Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МБОУ «Средняя школа №6» требованиям законодательства в сфере обработки персональных данных (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных в МБОУ «Средняя школа №6» (далее – образовательная организация) требованиям к защите персональных данных, установленным законодательством Российской Федерации.

1.3. Исполнение Положения обязательно для всех работников образовательной 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, определенных статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

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

**Внутренний аудит соответствия обработки персональных данных** – контроль соответствия обработки персональных данных в образовательной организации требованиям законодательства в сфере обработки персональных данных, проводимый специализированными организациями, привлекаемыми образовательной организацией по договорам оказания услуг в соответствии с Положением и другими локальными нормативными актами организации.

**2. Порядок проведения внутреннего контроля**

2.1. Внутренний контроль соответствия обработки персональных данных осуществляется комиссией, утверждаемой руководителем образовательной организации.

2.2. Внутренний контроль может быть внеплановым по решению комиссии, если есть фактические основания полагать, что процедура обработки персональных данных в образовательной организации не соответствует требованиям законодательства Российской Федерации.

2.3. Состав комиссии утверждается руководителем образовательной организации.

2.4. Внутренний контроль может 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 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. 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 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 образовательной 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. Внутренний контроль не может длиться больше 10 рабочих дней. Срок мероприятия может быть продлен распорядительным актом руководителя образовательной 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.

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 руководителе образовательной организации, если иное не установлено распорядительным актом руководителя образовательной организации.

3.5. Акты внутреннего контроля хранятся в запирающемся шкафу в кабинете заместителя руководителя образовательной организации.

#### **4. Порядок проведения внутреннего аудита**

4.1. Внутренний аудит соответствия обработки персональных данных проводится в случаях, когда образовательная организация не может объективно оценить соответствие обработки персональных данных в образовательной организации требованиям законодательства в сфере обработки персональных данных.

4.2. Внутренний аудит организуется на основании распорядительного акта руководителя образовательной 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 руководитель образовательной 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 руководителя образовательной 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 заместителя руководителя образовательной организации.

Приложение  
к Положению о внутреннем контроле и (или) аудите  
соответствия обработки персональных данных  
в МБОУ «Средняя школа №6» требованиям законодательства  
в сфере обработки персональных данных

Акт №\_\_\_\_\_ от \_\_\_\_\_

**внутреннего контроля соответствия обработки персональных данных  
в МБОУ «Средняя школа №6» требованиям законодательства  
в сфере обработки персональных данных**

Комиссия МБОУ «Средняя школа №6» в составе:

Заместителя директора по безопасности .....

Секретаря .....

Системного администратора .....

провела внутренний контроль соответствия обработки персональных данных в МБОУ «Средняя школа №6» требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на \_\_\_\_\_ учебный год, утвержденным приказом директора МБОУ «Средняя школа №6» от \_\_\_\_\_ № \_\_\_\_\_.

В ходе контрольных мероприятий проверены:

- документы, определяющие основания обработки персональных данных;
- утвержденный перечень работников МБОУ «Средняя школа №6», имеющих доступ к персональным данным в силу своих служебных обязанностей;
- своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в МБОУ «Средняя школа №6», в связи с достижением целей обработки или утраты необходимости в достижении этих целей;
- отсутствие неправомерно размещенных персональных данных граждан на сайте МБОУ «Средняя школа №6» и иных общедоступных местах;
- ...

Выявленные нарушения:

1. Политика обработки персональных данных МБОУ «Средняя школа №6» не соответствует требованиям законодательства – нет положений о согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2. <...>

Меры по устранению нарушений:

1. Необходимо внести изменения в Политику обработки персональных данных МБОУ «Средняя школа №6» и привести нормы о согласии на обработку персональных данных в соответствие с действующим законодательством.

2. <...>

Срок устранения нарушений: \_\_\_\_\_

Ответственный за исполнение: \_\_\_\_\_

Подписи членов комиссии:

Заместитель директора по безопасности .....

Секретарь .....

Системный администратор .....