

**ПРАВИЛА
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В МБДОУ №29
ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ,
УСТАНОВЛЕННЫМ ФЕДЕРАЛЬНЫМ ЗАКОНОМ
ОТ 27.07.2006 № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»,
ПРИНЯТЫМИ В СООТВЕТСТВИИ С НИМ НОРМАТИВНЫМИ
ПРАВОВЫМИ АКТАМИ И ЛОКАЛЬНЫМИ АКТАМИ ОПЕРАТОРА**

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в Муниципального бюджетного дошкольного образовательного учреждения детский сад №29 (далее – МБДОУ №29) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора (далее - Правила), определяют порядок действий, направленных на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в МБДОУ №29, а также цели, основания и виды внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 21.03.2012 № 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», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3. Целью осуществления внутреннего контроля соответствия обработки персональных данных в МБДОУ №29 требованиям к защите персональных данных (далее - внутренний контроль) является соблюдение в управлении образования законодательства Российской Федерации в области

персональных данных, в том числе требований к защите персональных данных.

4. Внутренний контроль подразделяется на плановый и внеплановый.

5. Внутренний контроль осуществляется лицом, ответственным за организацию обработки персональных данных, либо комиссией, образуемой приказом МБДОУ №29, в состав которой входят лицо, ответственное за организацию обработки персональных данных, и работники, уполномоченные на обработку персональных данных.

6. Плановый внутренний контроль проводится на основании плана, утвержденного МБДОУ №29. Периодичность планового контроля - не реже одного раза в год.

Срок проведения планового внутреннего контроля составляет не более 20 рабочих дней.

7. Внеплановый внутренний контроль проводится по решению руководителя МБДОУ №29:

- на основании поступившего в МБДОУ №29 в письменной форме или в форме электронного документа заявления субъекта персональных данных о нарушении законодательства в области персональных данных, а также устного обращения;

- в связи с проведением в МБДОУ №29 государственного контроля (надзора) за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных.

Внеплановый внутренний контроль может проводиться на основании решения руководителя МБДОУ №29.

8. Внеплановый внутренний контроль должен быть завершен не позднее чем через месяц со дня принятия решения о его проведении.

9. Результаты внутреннего контроля оформляются в виде акта по форме согласно приложению № 1 к настоящим Правилам.

9.1. При выявлении в ходе внутреннего контроля нарушений в акте отражается перечень мероприятий по устранению выявленных нарушений, ответственный за устранение нарушений и сроки их устранения.

9.2. Акт составляется в двух экземплярах, подписывается председателем и членами комиссии. С Актом под подпись знакомится сотрудник, в отношении которого проводилась проверка.

9.3. Акты хранятся у ответственного за организацию обработки персональных данных в течение текущего года. Уничтожение Актов проводится ответственным за организацию обработки персональных данных; самостоятельно в январе следующего за проверочным годом.

10. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, руководителю МБДОУ №29 докладывает лицо, ответственное за организацию обработки персональных данных.

11. В отношении персональных данных, ставших известными лицу, ответственному за организацию обработки персональных данных, или

членам комиссии в ходе проведения внутреннего контроля, соблюдается конфиденциальность и обеспечивается безопасность при их обработке.

12. Тематика внутреннего контроля:

12.1. При осуществлении внутреннего контроля соответствия обработки персональных данных с использованием средств автоматизации установленным требованиям проводится проверка:

- соответствия полномочий пользователя матрице доступа;
- соблюдения пользователями информационной системы (ИС) парольной политики;
- соблюдения пользователями ИС антивирусной политики;
- соблюдения пользователями ИС правил работы с носителями информации;
- соблюдения порядка доступа в помещения, где расположены элементы ИС;
- соблюдения порядка резервирования баз данных и хранения резервных копий;
- соблюдения порядка работы со средствами защиты информации;
- знаний пользователей ИС о своих действиях во внештатных ситуациях;
- иных вопросов.

12.2. При осуществлении внутреннего контроля соответствия обработки персональных данных без использования средств автоматизации установленным требованиям проводится проверка:

- хранения бумажных носителей с персональными данными;
- соблюдения доступа к бумажным носителям с персональными данными;
- соблюдения доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

12.3. В ходе внутреннего контроля могут обрабатываться вопросы:

- соблюдения общих принципов обработки персональных данных в управлении образования;
- соответствия локальных актов в области персональных данных управления образования действующему законодательству Российской Федерации;
- актуальности перечня информационных систем в МБДОУ №29;
- актуальности перечней персональных данных, используемых для решения задач и функций сотрудниками МБДОУ №29 и необходимости обработки персональных данных в информационных системах персональных данных МБДОУ №29;
- актуальности персональных данных, содержащихся в информационных системах персональных данных;

– актуальности перечня должностей работников МБДОУ №29, уполномоченных на осуществление обработки персональных данных, либо осуществление доступа к ним;

– соблюдения прав субъектов персональных данных, чьи персональные данные обрабатываются в МБДОУ №29;

– порядка взаимодействия с субъектами персональных данных, чьи персональные данные обрабатываются в МБДОУ №29, в том числе соблюдения сроков, предусмотренных действующим законодательством, в области персональных данных, соблюдения требований к уведомлениям, порядка разъяснения субъектам персональных данных необходимой информации, порядка реагирования на обращения субъектов персональных данных, порядка действий при достижении целей обработки персональных данных и отзыве согласий субъектами персональных данных;

– наличия необходимых согласий субъектов персональных данных, чьи персональные данные обрабатываются в МБДОУ №29;

– иных вопросов.

13. Все внутренние проверки фиксируются в Журнале учета мероприятий по контролю над соблюдением режима защиты информации, по форме согласно приложению к приказу МБДОУ №29 администрации города Коврова «Об утверждении документов по защите информации».

АКТ

о результатах проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора

в _____
название структурного подразделения

МБДОУ №29

«__» _____ 20__ г.

№ _____

г. Ковров

Комиссией в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

Проведена проверка _____

предмет проверки

Проверка осуществлялась в соответствии с требованиями _____

название документа

В ходе проверки установлено, что _____

Выявленные

нарушения:

Меры по устранению нарушений: _____

Ответственным за устранение нарушений назначен: _____ Срок устранения нарушений: _____

Председатель комиссии

_____ *подпись*

_____ *расшифровка подписи*

Члены комиссии

_____ *подпись*

_____ *расшифровка подписи*

_____ *подпись*

_____ *расшифровка подписи*

_____ *подпись*

_____ *расшифровка подписи*

Руководитель структурного
подразделения

_____ *подпись*

_____ *расшифровка подписи*

