муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад общеразвивающего вида № 19 п. Новый Надеждинского района»

П Р И К А З

от 16.01.2023 года п. Новый № 28/2-оа

О внутреннем контроле и (или) аудите соответствия обработки персональных данных в МБДОУ ДСОВ № 19 (Анисимова 90 Б) требованиям законодательства в сфере обработки персональных данных

В соответствии с п. 4 части 1 статьи 18.1 Федерального закона от 27.07.2006 №152-ФЗ (в редакции от 01.03.2023)

ПРИКАЗЫВАЮ:

1. Утвердить Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МБДОУ ДСОВ № 19 (Анисимова 90 Б) требованиям законодательства в сфере обработки персональных данных (Приложение 1).

2. Создать и утвердить комиссию по проверке обработки персональных данных в МБДОУ ДСОВ № 19 в следующем составе:

Председатель - Матафонова П.А., заведующий.

Члены комиссии – Кукушкина Т.В., методист;

- Панькова И.Л., ответственный за безопасность;

- Сиденко И.О., секретарь учебной части.

3. Утвердить План-график внутреннего контроля работы с персональными данными (Приложение 2).

4. Комиссии по проведению внутреннего контроля соответствия обработки персональных данных:

- провести мероприятия внутреннего контроля в соответствии с планом-графиком, указанным в пункте 3 настоящего приказа, и положением о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МБДОУ ДСОВ № 19 требованиям законодательства в сфере обработки персональных данных;
- представить итоги внутреннего контроля в срок, указанный в плане-графике мероприятий внутреннего контроля соответствия обработки персональных данных на 2023 год.

5. Секретарю учебной части Сиденко И.О. ознакомить с настоящим приказом работников под подпись в срок до 20.01.2023.

6. Контроль за исполнением настоящего приказа оставляю за собой.

Заведующий МБДОУ ДСОВ № 19 П.А. Матафонова

С приказом работники ознакомлены:

_____
_____
_____

Приложение 1 к приказу МБДОУ ДСОВ № 19
от 16.01.2023 № 28/2-оа

Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в МБДОУ ДСОВ № 19 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 МБДОУ ДСОВ № 19 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 МБДОУ ДСОВ № 19 (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 по плану мероприятий внутреннего контроля, утверждаемому ежегодно руководителем образовательной организации.

2.2. Мероприятия внутреннего контроля могут быть внеплановыми 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. Мероприятия внутреннего контроля могут 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 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 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. Мероприятие внутреннего контроля 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 комиссий 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 образовательной 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 руководителе образовательной организации, если иное не установлено распорядительным актом руководителя образовательной организации.

3.5. Акты внутреннего контроля, докладные записки по итогам контрольных мероприятий 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 Центр образования № 1 требованиям законодательства
в сфере обработки персональных данных

Акт №____ от _____

внутреннего контроля соответствия обработки персональных данных
в МБДОУ ДСОВ № 19 требованиям законодательства
в сфере обработки персональных данных

Комиссия МБДОУ ДСОВ № 19 в составе:

Заведующий

Заместитель заведующего по безопасности _____

Методист _____

Секретарь _____

провела внутренний контроль соответствия обработки персональных данных в МБДОУ ДСОВ № 19 требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на 2022/2023 учебный год, утвержденным приказом заведующего МБДОУ ДСОВ № 19 от _____ № _____.

В ходе контрольных мероприятий проверены:

- документы, определяющие основания обработки персональных данных;
- утвержденный перечень работников МБДОУ ДСОВ № 19, имеющих доступ к персональным данным в силу своих служебных обязанностей;
- своевременность мероприятий по уничтожению либо обезличиванию персональных данных, обрабатываемых в МБДОУ ДСОВ № 19, в связи с достижением целей обработки или утраты необходимости в достижении этих целей;
- отсутствие неправомерно размещенных персональных данных граждан на сайте МБДОУ ДСОВ № 19 и иных общедоступных местах;
- …

Выявленные нарушения:

1. Политика обработки персональных данных МБДОУ ДСОВ № 19 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 МБДОУ ДСОВ № 19 и привести нормы о согласии на обработку персональных данных в соответствие с действующим законодательством.

2. <…>

Срок устранения нарушений: 07.10.2022.

Ответственный за исполнение: _____

Подписи членов комиссии:

Заведующий _____

Заместитель заведующего по безопасности _____

Методист _____

Секретарь _____

Приложение 2 к приказу МБДОУ ДСОВ № 19
от 16.01.2023 № 28/2-оа

План-график мероприятий внутреннего контроля соответствия обработки персональных данных на 2023 год

Мероприятие	Ответственный	Срок исполнения
Проверка соблюдения правил доступа к персональным данным	Методист, ответственный за обработку персональных данных; ответственный по безопасности	01.02.2023, 01.03.2023, 01.04.2023, 04.05.2023, 01.06.2023 22.09.2023, 22.10.2023, 22.11.2023, 22.12.2023
Проверка соблюдения режима защиты		
Проверка выполнения антивирусной политики	Методист, ответственный за обработку персональных данных; ответственный по безопасности	23.03.2023, 23.06.2023, 23.09.2023, 23.12.2023
Проверка обновления ПО и единообразия применяемого ПО на всех устройствах, используемых при обработке персональных данных		
Проверка актуальности локальных нормативных актов в сфере обработки персональных данных	Секретарь учебной части	10.01.2023, 16.05.2023, 30.09.2023
Рассмотрение итогов мероприятий внутреннего контроля на совещании при Заведующем	Методист, ответственный за обработку персональных данных; ответственный по безопасности	