МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД № 32 «РОСИНКА»

ПРИКАЗ

10.05.2017г. № 14-ОД

х.Соленое Озеро

«Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных»

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением 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 и муниципальными органами», Приказом ФСТЭК РФ от 05.02.2010 № 58 «Об утверждении Положения о методах и способе защиты информации в информационных системах персональных данных»

П Р И К А З Ы В А Ю:

1.Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных (Приложение № 1).

- состав комиссии по проведению внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных согласно (Приложению 2);

2. Утвердить Положение о комиссии по проведению внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных (приложению 3);

3.Утвердить План внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных(Приложение 4);

4.Утвердить Протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение 5);

5.Утвердить Контрольный лист по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных (Приложение 6.).

6.Н.А.Марковой, председателю ПО, ознакомить работников МКДОУ ДС № 32 «Росинка» х.Соленое Озеро с указанными изменениями в срок до 31.05.2017г.

7. Контроль за исполнением приказа оставляю за собой.

Заведующий МКДОУ ДС № 32
«Росинка» х.Соленое Озеро А.П.Коваленко

Приложение 1
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных
приказ № 14 –ОД от 10.05.2017г.

Правила осуществления внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных

1.Настоящими Правилами определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок проведения внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее — Федеральный закон «О персональных данных»), принятыми в соответствии с ним правовыми актами (далее – ПДн).

2.Настоящие Правила разработаны в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и принятыми в соответствии с ними нормативными правовыми актами.

3.В настоящих Правилах используются основные понятия в значениях, определенных статьей 3 Федерального закона «О персональных данных».

4.Внутренний контроль соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных (далее — внутренний контроль) осуществляется комиссией по проведению внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных (далее – комиссия) путем проведения проверок. Состав комиссии утверждается приказом МКДОУ ДС № 32 «Росинка» х.Соленое Озеро.

5.Проверки по предметам контроля, указанным в акте внутреннего контроля, согласно приложению к настоящим Правилам, 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 в следующих целях:

5.1.выполнения требований организационно-распорядительной документации по защите информации в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

5.2.оценка уровня осведомленности и знаний работников МКДОУ ДС № 32 «Росинка» х.Соленое Озеро в области обработки и защиты персональных данных;

5.3.оценка обоснованности и эффективности применяемых мер и средств защиты.

2.Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1.Проверки соответствия обработки ПДн установленным требованиям в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2.Регулярные контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План) и предназначены для осуществления контроля выполнения требований в области защиты информации в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро.

2.3Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн МКДОУ ДС № 32 «Росинка» х.Соленое Озеро. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.по результатам расследования инцидента информационной безопасности;

2.5.по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.6.по решению заведующего МКДОУ ДС № 32 «Росинка» х.Соленое Озеро.

3.Планирование контрольных мероприятий

. Проверки соответствия обработки персональных данных, установленных требованиям, проводятся один раз в год.

3.1.Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2.План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1.цели проведения контрольных мероприятий;

3.2.2.задачи проведения контрольных мероприятий,

3.2.3.объекты контроля (процессы, подразделения, информационные системы и т.п.);
3.2.4.состав участников, привлекаемых для проведения контрольных мероприятий;
3.2.5.сроки и этапы проведения контрольных мероприятий.
3.3.Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4.Оформление результатов контрольных мероприятий

4.1. Результаты проведенных проверок оформляются секретарем комиссии в виде акта внутреннего контроля, составленного по форме согласно Приложению к настоящим Правилам, который подписывается членами комиссии в количестве не менее 3-х человек и утверждается председателем комиссии, а в его отсутствие — заместителем председателя комиссии.

4.2. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости председатель комиссии докладывает на очередном совещании.

5.Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Проведение внеплановой проверки организуется председателем комиссии, а в его отсутствие — заместителем председателя комиссии в течение 3-х рабочих дней с даты поступления письменного заявления субъекта персональных данных о нарушении правил обработки персональных данных.

5.2. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

5.3. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро

Приложение 4
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям к
защите персональных данных
приказ № 14 –ОД от 10.05.2017г.

ПЛАН

внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПД	1 раз в квартал	1 раз в полгода	ответственный за обеспечение безопасности персональных данных
Контроль соблюдения режима защиты	1 раз в квартал	1 раз в полгода	Ответственный за обеспечение безопасности персональных данных
Контроль выполнения антивирусной политики	1 раз в квартал	1 раз в полгода	Ответственный за обеспечение безопасности персональных данных
Контроль выполнения парольной политики	1 раз в квартал	1 раз в полгода	Ответственный за обеспечение безопасности персональных данных
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	1 раз в квартал	1 раз в год	Ответственный за обеспечение безопасности персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПД	по необходимости	1 раз в полгода	Ответственный за обеспечение безопасности персональных данных
Контроль обновления ПО и единообразия применяемого ПО	1 раз в квартал	1 раз в полгода	Ответственный за обеспечение безопасности персональных данных

Контроль обеспечения резервного копирования	по необходимости	1 раз в полгода	Ответственный за обеспечение безопасности персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности ПД, а также предсказание появления новых, еще неизвестных, угроз	По необходимости	1 раз в год	Ответственный за обеспечение безопасности персональных данных
Поддержание в актуальном состоянии нормативно-организационных документов	Периодически	1 раз в полгода	Ответственный за обеспечение безопасности персональных данных

Приложение 5
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
приказ № 14 –ОД от 10.05.2017г.

ПРОТОКОЛ № ____

проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро

Настоящий Протокол составлен в том, что «__»_____201_ г.
_____ (комиссией)
(должность, Ф.И.О. сотрудника)
проведена проверка _____
(тема проверки)

Проверка осуществлялась в соответствии с требованиями:
_____
(название документа)
_____

В ходе проверки проверено:
_____
_____
_____

Выявленные нарушения:
_____
_____
_____
_____

Меры по устранению нарушений:
_____
_____

Срок устранения нарушений: _____

Председатель комиссии:
фамилия и инициалы / подпись / должность

Члены комиссии:
фамилия и инициалы / подпись / должность
фамилия и инициалы / подпись / должность

Приложение 2
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных
приказ № 14 –ОД от 10.05.2017г.

Состав комиссии
по проведению внутреннего контроля
соответствия обработки персональных данных
в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро
требованиям к защите персональных данных

ФИО - Должность _____ - председатель комиссии

ФИО - Должность _____ - заместитель председателя комиссии

ФИО - Должность _____ - секретарь комиссии

Члены комиссии:

ФИО - Должность _____

ФИО - Должность

Приложение 3
к Правилам осуществления внутреннего
контроля соответствия обработки персональных
данных требованиям к защите персональных данных
приказ № 14 –ОД от 10.05.2017г.

Положение о комиссии по проведению внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных

I. Общие положения

1.1. Положение о комиссии по проведению внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных (далее - Комиссия) определяет функции, состав, полномочия и порядок функционирования комиссии по проведению внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных.

1.2. Комиссия вносит заведующему предложения по вопросам обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро.

II. Основные функции Комиссии

2.1. Комиссия изучает вопросы деятельности **МКДОУ ДС № 32 «Росинка» х.Соленое Озеро**, связанных с обработкой персональных данных и их защитой.

2.2. Комиссия осуществляет внутренний контроль соответствия обработки персональных данных в **МКДОУ ДС № 32 «Росинка» х.Соленое Озеро** требованиям к защите персональных данных путем проведения проверок.

III. Порядок работы Комиссии

3.1. Основной формой работы Комиссии является проверка.

3.2. Заведующий **МКДОУ ДС № 32 «Росинка» х.Соленое Озеро** утверждает план проверки.

3.3. Секретарь Комиссии отвечает за подготовку проверок, оформляет акты внутреннего контроля соответствия обработки персональных данных требованиям защиты персональных данных, контролирует выполнение рекомендаций Комиссии по результатам проверок, готовит отчеты о работе Комиссии.

3.4. Заседания Комиссии проводятся по мере необходимости, но не реже одного раза в год.

3.5. Материалы к обсуждению на заседаниях Комиссии готовятся секретарем Комиссии.

3.6. По результатам заседаний Комиссии оформляются протоколы заседаний Комиссии, которые подписываются председателем Комиссии и секретарем Комиссии.

3.7. По результатам осуществления внутреннего контроля соответствия обработки персональных данных в МКДОУ ДС № 32 «Росинка» х.Соленое Озеро требованиям к защите персональных данных составляется акт внутреннего контроля соответствия обработки персональных данных, который подписывается членами Комиссии в количестве не менее 3-х человек и утверждается председателем Комиссии, а в его отсутствие - заместителем председателя Комиссии.

IV. Полномочия Комиссии

Комиссия имеет право:

- знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на нее задач;
- привлекать в установленном порядке специалистов, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы Комиссии, и выработки соответствующих рекомендаций и заключений;
- проводить проверку непосредственно на рабочих местах работников;
- вносить заведующему МКДОУ ДС № 32 «Росинка» х.Соленое Озеро предложения об устранении нарушений в деятельности МКДОУ ДС № 32 «Росинка» х.Соленое Озеро по вопросам, отнесенным к компетенции Комиссии.

V. Контроль за работой Комиссии

5.1. Комиссия подотчетна заведующему. Председатель Комиссии периодически, но не реже одного раза в год, отчитывается заведующему МКДОУ ДС № 32 «Росинка» х.Соленое Озеро об итогах работы Комиссии и реализации ее предложений и рекомендаций.

– Итоги работы Комиссии отражаются в годовых отчетах, представляемых заведующему МКДОУ ДС № 32 «Росинка» х.Соленое Озеро.

Приложение 6.
к Правилам осуществления внутреннего
контроля соответствия обработки персональных
данных требованиям к защите персональных данных
приказ № 14 –ОД от 10.05.2017г.

Контрольный лист по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите персональных данных № ____

Критерии проверки ИР.

Примечание:

1. Соответствие состава фактически собираемых и обрабатываемых персональных данных утвержденному перечню.

2.Соблюдение ограниченного доступа к персональным данным.

3. Соблюдение мер по обеспечению безопасности персональных данных:
3.1. Физическая защита материальных носителей персональных данных;
3.2.Защита персональных данных, обрабатываемых с помощью средств вычислительной техники;

4.Соблюдение порядка уточнения, блокирования и уничтожения персональных данных.

5. Контроль ведения журналов.

6.Организация хранения персональных данных/Соответствие хранения персональных данных.

7.Работа с обращениями субъектов персональных данных.

8. Соблюдение правил передачи персональных данных третьим лицам

(Фамилия И.О., должность, подпись)