МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР "ЦЕНТР РАЗВИТИЯ РЕБЁНКА - ДЕТСКИЙ САД № 231"

Подписано цифровой подписью: МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ГОРОД КРАСНОДАР "ЦЕНТР РАЗВИТИЯ РЕБЁНКА - ДЕТСКИЙ САД № 231"
Дата: 2022.02.14 11:20:41 +03'00'

«УТВЕРЖДАЮ»
Заведующий МАДОУ
МО г. Краснодар
«Центр - детский сад №231»

_____М.С. Варданян

«____» _____ 20___г.

ПРАВИЛА

ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

в муниципальном автономном дошкольном образовательном учреждении муниципального образования город Краснодар «Центр развития ребёнка – детский сад № 231»

г. Краснодар

1. Общие положения

1. Настоящие Правила определяют основания, форму и порядок осуществления в муниципальном автономном дошкольном образовательном учреждении муниципального образования город Краснодар «Центр развития ребенка - детский сад № 231» (далее – ДОО) внутреннего контроля соответствия обработки персональных данных, требованиям к защите персональных данных и политике оператора, в отношении обработки персональных данных, установленным Федеральным законом от 27.07.2006г. № 152-ФЗ «О персональных данных» и принятыми, в соответствии с ним нормативными правовыми актами.

2. Настоящие Правила разработаны в соответствии с:

- Федеральным законом РФ № 152-ФЗ от 27.07.2006г. № 152-ФЗ «О персональных данных» и принятыми, в соответствии с ним, нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных Постановлением Правительства РФ от 21 марта 2012 г. № 211;

- Федеральным законом РФ № 210-ФЗ от 27.07.2010г. «Об организации предоставления государственных и муниципальных услуг»;

- Постановлением Правительства Российской Федерации от 01.11.2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ от 27.07.2006г. № 152-ФЗ «О персональных данных».

4. Основанием для проведения внутреннего контроля являются требования Федерального закона № 152-ФЗ (часть 1, статья 18.1) и Постановления Правительства № 1119 (п. 17).

5. Внутренний контроль осуществляется путем проведения проверок, не реже 1 раза в год.

6. Проверку проводит Комиссия, назначенная приказом заведующего МАДОУ МО г. Краснодар «Центр – детский сад № 231» или на договорной основе, юридическое лицо (индивидуальный предприниматель), имеющее лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7. Состав Комиссии, не менее 3-х человек, включая лицо, ответственное за организацию обработки персональных данных. Все члены комиссии, при принятии решения, обладают равными правами.

8. Комиссия, при проведении проверки, обязана:

– провести анализ реализации мер, направленных на обеспечение выполнения ДОО обязанностей, предусмотренных Федеральным законом № 152-ФЗ (статья 18.1, статья 19) и принятыми, в соответствии с ним, локальными актами ДОО, определяющих его политику, в отношении обработки персональных данных;

– провести анализ выполнения ДОО требований, по определению и обеспечению уровня защищенности персональных данных, утвержденных Постановлением Правительства № 1119;

– провести анализ реализации ДОО организационных и технических мер, по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер, по обеспечению безопасности персональных данных, при их обработке в информационных системах персональных данных»;

– провести анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы;

– своевременно и в полной мере исполнять предоставленные полномочия по предупреждению, выявлению и пресечению нарушений требований к защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации;

– при проведении проверки соблюдать законодательство Российской Федерации, права и законные интересы ДОО.

9. Комиссия, при проведении проверки, вправе:

– запрашивать и получать необходимые документы (сведения), для достижения целей проведения внутреннего контроля;

– получать доступ к информационным системам персональных данных, в части касающейся ее полномочий;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой к нарушениям требований по защите персональных данных;

– вносить заведующему ДОО предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований по защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации.

10. При проведении проверки члены Комиссии не вправе:

– требовать представления документов и сведений, не относящихся к предмету проверки;

– распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки персональных данных требованиям по их защите:

2.1. Проверки соответствия обработки персональных данных, установленным требованиям в ДОО, разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически, в соответствии с утвержденным Планом проведения контрольных мероприятий, предназначенных для осуществления контроля выполнения требований, в области защиты информации в ДОО и направленных на постоянное совершенствование системы защиты персональных данных.

2.3. 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:

- по результатам расследования инцидента информационной безопасности;

- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

- по решению заведующего ДОО.

3. Оформление результатов контрольных мероприятий

3.1. По результатам проверки составляется Протокол проверки, который подписывается членами комиссии и представляется руководителю организации для принятия соответствующего решения.

3.2. В Протоколе отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации, в области защиты персональных данных, об их характере и о лицах, допустивших указанные нарушения.

3.3. Протокол должен содержать заключение о соответствии или несоответствии обработки персональных данных требованиям по защите персональных данных и политике ДОО, в отношении обработки персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми, в соответствии с ним, нормативными правовыми актами.

3.4. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения внутреннего контрольного мероприятия.

3.5. Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета событий информационной безопасности.

3.6. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в ДОО (приложение 2).

4. Порядок проведения плановых и внеплановых контрольных мероприятий

4.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности персональных данных, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных ДОО.

4.2. Лицо, ответственное за обеспечение безопасности персональных данных, не позднее чем за три рабочих дня до начала проведения

контрольных мероприятий, уведомляет все подразделения, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

4.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- соответствие полномочий Пользователя правилам доступа;

- соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции, по обеспечению безопасности персональных данных;

- соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в ДОО;

- соблюдение Порядка доступа в помещения ДОО, где ведется обработка персональных данных;

- знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки персональных данных, при возникновении внештатных ситуаций;

- знание Администраторами инструкций и регламентов по обеспечению безопасности информации в ДОО;

- порядок и условия применения средств защиты информации;

- состояние учета машинных носителей персональных данных;

- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

- проведенные мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- технические мероприятия, связанные со штатным и нештатным функционированием средств защиты;

- технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

Приложение 1

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 персональным данным	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных

персональных данных			_____ ___
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС СПО	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____ ___
Контроль обеспечения резервного копирования		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____ ___
Организация анализа и пересмотра имеющихся угроз безопасности персональных данных, а также предсказание появления новых, еще неизвестных, угроз		Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____ ___
Поддержание в актуальном состоянии нормативно-организационных документов		Ежемесячно	Ответственный за организацию обработки персональных данных в _____ ___
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	

Приложение 2

ПРОТОКОЛ № ____

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

Настоящий Протокол составлен в том, что (дата) комиссией ДОО (должность, Ф.И.О. сотрудников)

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: до _____

Председатель комиссии: _____

фамилия и инициалы / подпись / должность

Члены комиссии: _____

фамилия и инициалы / подпись / должность

_____

фамилия и инициалы / подпись / должность