Муниципальное бюджетное дошкольное образовательное учреждение детский сад общеразвивающего вида №13

ПРИКАЗ

от 11.01.2021 г. №8

п.Комсомольский

О создании Комиссии МБДОУ д/с ОВ №13 по проведению периодических проверок для осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям

Во исполнение требований Федерального закона №152-ФЗ от 27.07.2006 года «О персональных данных» и в соответствии с постановлением Правительства РФ от 21.03.2012 г.№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,

приказываю:

1.Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (Приложение №1).
2.Создать Комиссию МБДОУ д/с ОВ №13 по проведению периодических проверок для осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в следующем составе:
Председатель:
-Гуденко А.В.- воспитатель
Члены комиссии:
-Илюшина О.Г.- воспитатель
-Беспалова Ю.В.- воспитатель
3.Утвердить План внутреннего контроля соответствия обработки персональных данных установленным требованиям на 2021 год.
(Приложение №2).
4.Комиссии, в своей работе руководствоваться Планом внутреннего контроля соответствия обработки персональных данных установленным требованиям на 2021 год, Положением «О проведении внутреннего контроля соответствия обработки персональных данных установленным требованиям»
5.Контроль за исполнением настоящего приказа оставляю за собой

Заведующий МБДОУ _____ Л.И.Шостак

Шостак Людмила Ивановна Подписано цифровой подписью: Шостак Людмила Ивановна Дата: 2021.01.11 10:38:46 +03'00'

С приказом ознакомлены: Гуденко А.В. Беспалова Ю.В. Илюшина О.Г.

Приложение №1 к приказу №8 от 11.01.2021 года

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном бюджетном дошкольном образовательном учреждении детском саду общеразвивающего вида №13

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в муниципальном бюджетном дошкольном образовательном учреждении детском саду общеразвивающего вида № 13 (далее - Учреждение) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «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», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.3. Для обработки ПДн необходимых для предоставления государственных и муниципальных услуг в Учреждении используется информационные системы персональных данных:

- СБИС;
- 1С: Профсоюз;
-АИС «Сетевой регион. Образование» и «Е-Услуги.Образование»

(далее - ИСПДн) предназначенная для осуществления деятельности обработки персональных данных, согласно Положения об обработке персональных данных в Учреждении.

1.4. Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в Учреждении в соответствии с Трудовым кодексом Российской Федерации, используется ИСПДн-1С: Предприятие.

1.5. Пользователем ИСПДн (далее - Пользователь) является сотрудник

ответственный за работу в ИСПДН, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО. данным и средствам защиты информации (далее - СЗИ) ИСПДн.

1.6. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн Учреждения проводятся в следующих целях:

-проверка выполнения требований организационно-распорядительной документации по защите информации в Учреждении и действующего законодательства Российской Федерации **в** области обработки и защиты персональных данных;

-оценка уровня осведомленности и знаний работников Учреждения в области обработки и защиты персональных данных;

-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 Учреждении разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся заведующим периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План) и предназначены для осуществления контроля выполнения требований в области защиты информации в Учреждении.

2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн Учреждения.

2.4. Внеплановыеконтрольные 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;

-но результатам внешних контрольных мероприятий, проводимых регулирующими органами;

-но решению заведующего Учреждения.

3. ПЛАНИРОВ АННЕ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

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:

-цели проведения контрольных мероприятий;

-задачи проведения контрольных мероприятий,

-объекты контроля (процессы, подразделения, информационные системы и тли);

-состав участников, привлекаемых для проведения контрольных мероприятий;

-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. ОФ0РМЛЕНИЕ РЕЗУЛЬТАТОВ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале регистрации выявленных нарушений в сфере защиты персональных данных и иной конфиденциальной информации.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия разрабатывает справку, в которой 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, отчет передастся па рассмотрение заведующему Учреждения.

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

5.ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВЫХ И ВНЕПЛАНОВЫХ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

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

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполняться следующие проверки:

-соответствие полномочий Пользователя правилам доступа;

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

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

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

-знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;

-знание Администраторами инструкций и регламентов по обеспечению

безопасности информации в Учреждении;
-порядок и условия применения средств защиты информации;
-состояние учета машинных носителей персональных данных.
-наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;
-проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
-технические мероприятия, связанные с штатным и нештатным функционированием средств защиты;
-технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

Приложение
к Правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ д/с ОВ №13

Протокол
проведения внутренней проверки условий обработки персональных данных в МБДОУ д/с ОВ №13

Настоящий Протокол составлен в том, что __.__.202_ ответственным за организацию обработки персональных данных/комиссией по внутреннему контролю 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: _____.

Должность ответственного _____ И.О. Фамили

Приложение № 2
К приказу №8 от 11.01.2021 года

План
внутренних проверок условий обработки персональных данных в МДОУ д/с ОВ №13

№	Тема проверки	Нормативный документ, предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие полномочий пользователя правилам обработки персональных данных	Положение по защите персональных данных МДОУ, обрабатываемых в ИСПДн	ежегодно	Ответственный за организацию обработки персональных данных
2.	Соблюдение пользователями информационных систем персональных данных парольной политики	Положение по защите персональных данных МДОУ, обрабатываемых в ИСПДн	еженедельно	Ответственный за организацию обработки персональных данных
3.	Соблюдение пользователями информационных систем персональных данных антивирусной политики		еженедельно	Ответственный за организацию обработки персональных данных
4.	Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных	Список помещений МДОУ, в которых обрабатываются персональные данные и доступ к ним	ежегодно	Ответственный за организацию обработки персональных данных
5.	Соблюдение порядка резервирования баз данных и хранения резервных копий	Положение по защите персональных данных МДОУ, обрабатываемых в ИСПДн	еженедельно	Ответственный за организацию обработки персональных данных
6.	Соблюдение порядка работы со средствами защиты информации		ежегодно	Ответственный за организацию обработки персональных данных
7.	Знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях		ежегодно	Ответственный за организацию обработки персональных данных
8.	Хранение бумажных носителей с	Положение по защите персональных данных МДОУ, обрабатываемых без	ежегодно	Ответственный за организацию обработки

	персональными данными	использования средств автоматизации		персональных данных
9.	Доступ к бумажным носителям с персональными данными		ежегодно	Ответственный за организацию обработки персональных данных
10.	Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными	Положение по защите персональных данных МДОУ без использования средств автоматизации Список помещений МДОУ, в которых обрабатываются персональные данные и доступ к ним	ежегодно	Ответственный за организацию обработки персональных данных