Согласовано:
председатель ПК
_____ С.Б. Самойлик

Утверждаю:
заведующий МБДОУ д/с № 9
_____ Л.В.Новикова
Приказ № 135 от 07.08.2014 г.

МБДОУ Д/С ОВ № 9

Digitally signed by МБДОУ Д/С ОВ № 9
DN: UnstructuredName=2340014460-234001001-001 224138588, E=cbuo86168@yandex.ru, ИНН=002340014460, СНИЛС=01224138588, ОГРН=1022304241552, T=Заведующая, O=МБДОУ Д/С ОВ № 9, STREET="УЛ КРАСНАЯ, ДОМ 1", L=Первомайский, S=23 Краснодарский край, C=RU, G=Лилия Владимировна, SN=Новикова, CN=МБДОУ Д/С ОВ № 9
Reason: I am the author of this document
Location:
Date: 2021-07-24 09:42:01

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных работников и обучающихся МБДОУ д/с ОВ № 9

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных" (далее - Правила), разработаны с учетом Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных" и постановления Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных".

1.2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных в муниципальном бюджетном дошкольном образовательном учреждении детском саду общеразвивающего вида № 9 (далее - ДОУ) требованиям к защите персональных данных и действуют постоянно.

2. Тематика внутреннего контроля

1.3. Тематика проверок обработки персональных данных с использованием средств автоматизации.

1.3.1. Соблюдение пользователями информационных систем персональных данных ДОУ парольной политики:

1.3.1.1. Правил формирования пароля;

1.3.1.2. Правил ввода пароля;

1.3.1.3. Правил хранения пароля.

1.3.2. Соблюдение пользователями информационных систем персональных данных ДОУ антивирусной политики:

2.1.2.1. поддержка рабочего состояния антивирусного программного обеспечения;

2.1.2.2. своевременное обновление антивирусного программного обеспечения.

2.1.3. Соблюдение пользователями информационных систем персональных данных ДОУ Правил работы со съемными носителями персональных данных:

2.1.3.1. хранение съемных носителей в сейфе заведующего, запирающегося на ключ, доступ к которому разрешен только заведующему либо исполняющему его обязанности;

2.1.3.2. проверка съемного носителя на наличие вредоносных программ, перед каждым началом работы с ним;

2.1.3.3. исключение копирования с данного носителя файлов сомнительного содержания и установки нелицензионного программного обеспечения;

2.1.3.4. исключение передачи съемного носителя третьим лицам;

2.1.3.5. запрет на оставление съемного носителя включенным/выключенным без присмотра;

2.1.3.6. запрет на обработку информации, содержащейся на съемном носителе в присутствии третьих лиц;

2.1.3.7. запрет на вынос съемного носителя за пределы служебного помещения.

2.1.4. Соблюдение ответственными за криптографические средства защиты информации Правил работы с ними:

2.1.4.1. хранение криптографических средств в сейфе заведующего, запирающемся на ключ, расположенном в кабинете заведующего ДОУ;

2.1.4.2. исключение передачи криптографического средства третьим лицам;

2.1.4.3. запрет на оставление криптографического средства включенным/выключенным без присмотра;

2.1.4.4. запрет на вынос криптографического средства за пределы служебного помещения;

2.1.4.5. запрет на использование для электронной цифровой подписи открытых и закрытых ключей электронной цифровой подписи, если пользователю известно, что эти ключи используются или использовались ранее;

2.1.4.6. запрет на разглашение конфиденциальной информации, к которой пользователи допущены, средства ее защиты, в том числе сведения о криптографических средствах;

2.1.4.7. обязанность сообщать в орган криптографической защиты о ставших пользователям известными попытках третьих лиц получить сведения об используемых криптографических средствах;

2.1.4.8. обязанность немедленно уведомлять орган криптографической защиты о фактах утраты криптографического средства.

2.1.5. Соблюдение порядка доступа в ДОУ, где расположены элементы информационных систем персональных данных:

2.1.5.1. все элементы информационных систем хранятся в сейфе заведующего, запирающемся на ключ, расположенном в кабинете заведующего ДОУ.

2.1.6. Соблюдение порядка резервирования баз данных и хранения резервных копий:

2.1.6.1. наличие актуальных резервных копий;

2.1.6.2. поддержка рабочего состояния систем хранения резервных копий.

2.1.7. Знание пользователей информационных систем персональных данных алгоритма действий во внештатных ситуациях:

2.1.7.1. проведение анкетирования/опроса пользователя о порядке действий во внештатных ситуациях.

2.2. Тематика проверок обработки персональных данных без использования средств автоматизации.

2.2.1. Хранение бумажных носителей с персональными данными:

2.2.1.1. соблюдение хранения бумажных носителей, содержащих персональные данные, в закрываемых шкафах;

2.2.1.2. запрет передачи бумажных носителей, содержащих персональные данные, третьим лицам;

2.2.1.3. запрет выноса бумажных носителей, содержащих персональные данные, за пределы служебного помещения;

2.2.2. Доступ к бумажным носителям с персональными данными:

2.2.2.1. исключение возможности доступа к бумажным носителям, содержащим персональные данные, третьих лиц.

2.2.3. Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными:

2.2.3.1. все бумажные носители хранятся в индивидуальных ящиках каждого пользователя, расположенных в кабинетах;

2.2.3.2. соблюдение установленного соответствующим приказом ДОУ ограничения в кабинеты, где хранятся бумажные носители персональных данных.

3. Порядок проведения проверок условий обработки персональных данных

3.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям ДОУ организует один раз в шесть месяцев. План проверки (Приложение № 1) утверждается заведующим ДОУ.

3.2. Проверки проводятся по необходимости в соответствии с поручением заведующего ДОУ.

3.3. Проверки осуществляются заведующим ДОУ, ответственным за организацию обработки персональных данных.

3.4. Проверки осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

3.5. Результаты каждой проверки заносятся в акт проверки (приложение № 2).

3.6. При выявлении в ходе проверки нарушений в акте делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.7. Акты хранятся у ответственного за организацию обработки персональных данных в ДОУ.

3.8. Ответственный за организацию обработки персональных данных в ДОУ несет персональную ответственность за качество организации, подготовки и проведения проверки, объективность и обоснованность ее результатов, выводов и предложений, за осуществление контроля по устранению выявленных нарушений и недостатков в ходе проверки.

Приложение № 1

План внутренних проверок условий обработки персональных данных МБДОУ д/с ОВ № 9

N	Тема проверки	Срок проведения
1	Соблюдение пользователями ИСПДн парольной политики	
2	Соблюдение пользователями ИСПДн антивирусной политики	
3	Соблюдение пользователями ИСПДн Правил работы со съемными носителями, на которых содержится информация о персональных данных	
4	Соблюдение пользователем Правил работы с криптографическими средствами защиты информации	
5	Соблюдение порядка доступа в помещения, в которых расположены элементы ИСПДн	
6	Соблюдение порядка резервирования баз данных и хранения резервных копий	
7	Соблюдение условий хранения бумажных носителей, содержащих информацию о персональных данных	
8	Соблюдение условий доступа к бумажным носителям, содержащим информацию о персональных данных	

Приложение № 2

Акт проведения внутренней проверки условий обработки персональных данных МБДОУ д/с ОВ № 9

Настоящий Акт составлен в том, что __.__.20____ ответственным за организацию обработки персональных данных проведена проверка

тема проверки _____.

В ходе проверки проверено:

_____

_____

_____

_____

_____.

Выявленные нарушения:

_____

_____

_____.

Меры по устранению нарушений:

_____
_____.

Срок устранения нарушений:

_____.

Должность Ответственного _____ И.О.Фамилия