ПРИНЯТО
Общим собранием работников
МБДОУ «Детский сад № 97» г.о. Самара
Протокол №_____
«_04_» _октября_ 20_19_г.

УТВЕРЖДЕНО
Заведующим МБДОУ
«Детский сад № 97» г.о. Самара
_____ Г.Н. Нилова
«_04_» _октября_ 20_19_ г.

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад общеразвивающего вида № 97 городского округа Самара

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 «Детский сад общеразвивающего вида № 97» городского округа Самара (далее – ДОУ), 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.

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 ПД сотрудников (получения, обработки, использования, передачи, хранения и т.д.), гарантии конфиденциальности сведений о работнике, предоставленных работником работодателю; права работника по защите его персональных данных; ответственность лиц за невыполнение норм, регулирующих обработку и защиту персональных данных работника.

Пользователь ПД (далее – пользователь) является сотрудник ДОУ, участвующий в рамках выполнения своих функциональных обязанностей в процессе автоматизированной обработки ПД и имеющий доступ к средствам, данным и средствам защиты информации (далее – СЗИ).

1.4. Контрольные мероприятия за обесп5чением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ДОУ проводятся в следующих целях:

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

1.14.2. оценка уровня осведомленности и знаний работников ДОУ в области обработки и защиты персональных данных;

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

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПД требованиям к защите ПД:

2.14. Проверки соответствия обработки ПД установленным требованиям в ДОУ разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.15. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий и предназначены для осуществления контроля выполнения требований в области защиты информации в ДОУ.

2.16. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий и направлены на постоянное совершенствование системы защиты персональных данных.

2.17. 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:

2.17.3. по результатам расследования инцидента информационной безопасности;

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

3. Планирование контрольных мероприятий

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

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

3.15.3. цели проведения контрольных мероприятий;

3.15.4. задачи проведения контрольных мероприятий,

3.15.5. объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.15.6. состав участников, привлекаемых для проведения контрольных мероприятий;

3.15.7. сроки и этапы проведения контрольных мероприятий.

3.16. Общий срок контрольных мероприятий не должен превышать трех рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на пять рабочих дней, соответствующие изменения отображаются в отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

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

4.3. описание проведенных мероприятий по каждому из этапов;

4.4. перечень и описание выявленных нарушений;

4.5. рекомендации по устранению выявленных нарушений;

4.6. заключение по итогам проведения внутреннего контрольного мероприятия.

4.7. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в администрации.

Порядок проведения плановых и внеплановых контрольных мероприятий

4.8. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПД, также по его ходатайству к проведению контрольных мероприятий могут привлекаться представители ДОУ, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных администрации.

4.9. 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 ПД.

– Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в администрации.

– Соблюдение Порядка доступа в помещения ДОУ, где ведется обработка персональных данных.

– Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций.

– Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в администрации.

– Порядок и условия применения средств защиты информации.

– Состояние учета машинных носителей персональных данных.

– Наличие (отсутствие) фактов несанкционированного доступа к ПД и принятие необходимых мер.

– Проведенные мероприятия по восстановлению ПД, 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 № 1

ПРОТОКОЛ № ____
проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных
в _____

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:

_____

Члены комиссии: _____

_____ ___

_____