Государственное казенное дошкольное образовательное учреждение детский сад № 25 «Солнышко»

УТВЕРЖДЕНЫ

Приказом заведующего
ГКДОУ д/с № 25 «Солнышко»
от 26.01.2021 г. № 03-12/48-1

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных (далее – Правила) устанавливают основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных (далее - ПД) требованиям, установленным в Государственном казенном дошкольном образовательном учреждении детском саду № 25 «Солнышко» (далее – Учреждение).

1.2. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации в области обработки и защиты ПД и иными правовыми актами, принимаемыми в соответствии с данным законодательством (далее – законодательство в сфере персональных данных).

1.3. Целями осуществления внутреннего контроля являются:

оценка общего состояния выполнения Учреждением требований по обработке и защите ПД, закрепленных законодательно, а также в локальных актах Учреждения;

выявление и предотвращение нарушений законодательства в сфере персональных данных.

1.4. Проверки проводятся комиссией по обеспечению безопасности ПД (далее – Комиссией), создаваемой приказом руководителя Учреждения.

В проведении проверки не может участвовать сотрудник, прямо или косвенно заинтересованный в ее результатах.

1.5. Члены Комиссии, получившие доступ к ПД субъектов ПД в ходе проведения проверки, обеспечивают конфиденциальность ПД субъектов ПД, не раскрывают третьим лицам и не распространяют ПД без согласия субъекта ПД.

2. Порядок осуществления внутреннего контроля

2.1. Внутренний контроль соответствия обработки ПД установленным требованиям (далее – внутренний контроль) осуществляется Учреждением путем проведения проверок соблюдения требований законодательства в сфере ПД.

2.2. Проверки разделяются на:

- регулярные;
- плановые;
- внеплановые.

2.3. Регулярные контрольные мероприятия проводятся ответственным лицом за безопасность обработки персональных данных периодически в соответствии с утвержденным Планом

проведения контрольных мероприятий (далее – План) **(Приложение 1)** и предназначены для осуществления контроля выполнения требований в области защиты информации в Учреждении.

2.4. Плановые проверки проводятся не реже одного раза в год.

2.5. Непосредственно перед началом проведения плановой проверки, за 10 (десять) рабочих дней, ответственным за организацию обработки ПД направляются уведомления руководителям структурных подразделений, в которых планируется проведение внутреннего контроля.

2.6. Внеплановые внутренние проверки могут проводиться в следующих случаях:

по результатам расследования выявленных нарушений требований законодательства в сфере ПД;

по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов ПД.

2.7. Проверка представляет собой комплекс мероприятий, который состоит из следующих этапов:

подготовка к проведению проверки;

сбор свидетельств проверки;

анализ соответствия контрольным параметрам;

подготовка заключения по проверке.

2.8. В ходе подготовки к проведению проверки Комиссия определяет:

границы и описание области, подвергающейся проверки;

перечень контрольных параметров;

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

состав участников, привлекаемых для проведения проверки;

сроки и этапы проведения проверки.

2.9. Типовой перечень контрольных параметров приведен в приложении 2 к настоящим Правилам**.**

2.10. Сбор свидетельств проверки включает:

анализ организационно-распорядительных и регламентирующих документов по обработке и защите ПД;

опрос персонала, участвующего в процессах обработки ПД, обслуживании и эксплуатации информационных систем ПД.

2.11. Проверки проводятся Комиссией непосредственно на месте обработки ПД путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки ПД.

2.12. Свидетельства проверки сопоставляются с контрольными параметрами для формирования заключения по проверке.

2.13. Общий срок проверки не должен превышать 20 (двадцати) рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более чем на 10 (десять) рабочих дней.

3. Права Комиссии при проведении проверки

3.1. Комиссия для реализации своих полномочий имеет право:

запрашивать у сотрудников Учреждения необходимую информацию;

принимать меры по устранению выявленных нарушений выполнения требований к защите ПД в Учреждении;

вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности ПД при их обработке;

вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПД.

4. Порядок фиксирования результатов проверки

4.1. Факт проведения проверок и результаты проверки фиксируются в журнале проведения проверок **(Приложение 3).**

4.2. По результатам проверки Комиссией, при необходимости, проводится заседание. Решения, принятые на заседаниях Комиссии, оформляются протоколом **(Приложение 4).**

4.3. В целях контроля устранения выявленных нарушений Комиссия проводит повторную проверку.

Приложение 1

ПЛАН ПРОВЕДЕНИЯ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ
по выполнению требований к обработке и защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	еженедельно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты	еженедельно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения антивирусной политики	1 раз в полгода	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения парольной политики	еженедельно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обеспечения резервного копирования	еженедельно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Поддержание в актуальном состоянии нормативно-организационных документов	1 раз в полгода	Ответственный за организацию обработки ПДн

Приложение 2

ПЕРЕЧЕНЬ
контрольных параметров проверок в области обработки и обеспечения безопасности персональных данных (типовой)

№ п/п	Контрольные параметры и объекты проверок
1.	Соответствие установленных в перечне персональных данных категорий персональных данных фактически обрабатываемым в Учреждении
2.	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3.	Подтверждение факта ознакомления с локальными актами Учреждения в области обработки и обеспечения безопасности персональных данных
4.	Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных
5.	Наличие законных целей и оснований обработки всех категорий персональных данных
6.	Выборочные проверки сотрудников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
7.	Соблюдение сроков хранения и порядка уничтожения персональных данных
8.	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных
9.	Необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных

Приложение 3

Форма

ЖУРНАЛ
проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

№	Дата проведения проверки	Основание проверки	Заключение по проверке (кратко)	Подпись председателя Комиссии	Примечание

Приложение 4

ПРОТОКОЛ № ____

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

Настоящий Протокол составлен в том, что «_» _____202_ 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