Приложение

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Центр развития ребёнка – детский сад № 11 «Рябинушка» города Заринска

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 «Центр развития ребёнка – детский сад № 11 «Рябинушка» города Заринска (далее Учреждение) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства РФ 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 ФЗ РФ от 07.07.2006 № 152-ФЗ «О персональных данных», ФЗ РФ от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21.03.2012 № 211.

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

- СБИС;
- 1С: Предприятие;
- АИС «Сетевой регион. 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 РФ, используется ИСПДн – 1С: Предприятие.

1.5. Пользователем ИСПДн (далее – Пользователь) является сотрудник ответственный за работу с 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 РФ по обработке персональных данных в ИСПИДн Учреждения проводятся в следующих целях:

- проверка выполнения требований организационно – распорядительной документации по защите информации в Учреждении и действующего законодательства РФ 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

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, приложение 1) 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. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности. Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующем случае:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению Заведующего Учреждения.

3. Планирование 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 т.п.);
- 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 10 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 фиксируются в журнале регистрации выявленных нарушений в сфере защиты персональных данных и иной конфиденциональной информации.

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

- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- описание проведенных мероприятий по каждому из этапов;
- заключение по итогам проведения внутреннего контрольного мероприятия;
- отчет передается на 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 1).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспе-

чение безопасности персональных данных информационных систем персональных данных Учреждения.
5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за 3 рабочих дня до начала проведения контрольных мероприятий уведомляет всех сотрудников, 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 положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;
- знание 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;
- проведение мероприятий по восстановлению ПДн, 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 подсистемы 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 ПДн	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 ПДн		ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обновления ПО	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 пересмотра имеющихся угроз безопасности ПДн		ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Поддержание в актуальном состоянии нормативно - организационных документов		ежемесячно	Ответственный за организацию обработки ПДн в Учреждении

Приложение 2

ПРОТОКОЛ

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

Настоящий Протокол составлен в том, сто _____ 20 ____ г.

_____

_____(комиссией)

(должность, ФИО сотрудника)

Проведена проверка

_____

_____

(тема проверки)

Проверка осуществлялась в соответствии с требованиями _____

_____

_____

(название документа)

В ходе проверки проверено: _____

_____

_____

_____

_____

Выявлены нарушения:_____

_____

_____

_____

_____

_____

Меры по устранению нарушений: _____

_____

_____

_____

_____

Срок устранения нарушений: _____

_____

_____

Председатель комиссии_____

Члены комиссии _____

_____

_____

_____

_____