Утверждаю
Заведующий МДОУ детский сад
комбинированного вида № 69
Малхасян Джульетта Размиковна
Подписано цифровой подписью: Малхасян Джульетта Размиковна
Дата: 2024.02.09 11:47:10 +03'00'
Приказ № 5\16 от 09.01.2024 года

Должностная инструкция
ответственного лица за организацию обработки персональных данных работников, родителей (законных представителей) воспитанников муниципального дошкольного образовательного бюджетного учреждения детского сада комбинированного вида № 69 муниципального образования городской округ город-курорт Сочи Краснодарского края

1. Общие положения

1.1. Данная инструкция определяет основные обязанности и права ответственного за организацию обработки персональных данных МДОУ детский сад комбинированного вида № 69 муниципального образования городской округ город-курорт Сочи Краснодарского края (далее - Учреждение).
1.2. Ответственный за организацию обработки персональных данных является штатным сотрудником учреждения и назначается приказом заведующей.
1.3. Решение вопросов организации защиты персональных данных в Учреждении входит в прямые служебные обязанности ответственного за организацию обработки персональных данных.
1.4. Ответственный за организацию обработки персональных данных обладает правами доступа к любым носителям персональных данных учреждения.

2. Термины и определения.

2.1. Автоматизированное рабочее место (АРМ)- персональный компьютер и подключенные к нему перифирийные устройства – принтер, сканер, многофункциональные устройства и т.д.
2.2. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст.3 ФЗ РФ от 27.07.2006г. № 152-ФЗ «О персональных даных»).
2.3. Доступ к информации – возможность получения информации и ее использования (ст. 2 ФЗ РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»).
2.4. Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.
2.5. Информация—сведения (сообщения, данные) независимо от формы их представления (ст 2 ФЗ РФ от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»).
- **Информационная система персональных данных (ИПДн**) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку

информационных технологий и технических средств *(ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

- **Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.
- **Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.
- **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*
- **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*
- **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
- **Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (*ст. 19 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»*).
- **Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (*ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).*

• ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

Ответственный за организацию обработки персональных данных обязан:

- Знать перечень и условия обработки персональных данных в Учреждении.
- Знать и предоставлять на утверждение заведующему изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей.
- Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.
- Осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения.
- Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.
- Реагировать на попытки несанкционированного доступа к информации в установленном ст.4 настоящей Инструкции порядке.
- Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

- Контролировать оперативное внесение изменений в конфигурацию технических средств ИСПДн, требовать отражения соответствующих изменений в «Техническом паспорте информационной системы персональных данных».
- По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПДн и правилам обработки персональных данных.
- Проводить занятия и инструктажи с сотрудниками и руководителями структурных подразделений о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.
- Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.
- Контролировать соблюдение сотрудниками локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.
- Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.
- Организовать учет обращений субъектов персональных данных, контролировать заполнение «Журнала учета обращений субъектов персональных данных» (Приложение 1).
- Представлять интересы Учреждения при проверках надзорных органов в сфере обработки персональных данных.
- Знать законодательство РФ о персональных данных, следить за его изменениями.
- Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

- ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

- К попыткам несанкционированного доступа относятся:
- сеансы работы с персональными данными незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;
- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.
- При выявлении факта несанкционированного доступа ответственный за организацию обработки персональных данных обязан:
- прекратить несанкционированный доступ к персональным данным;
- доложить заведующему Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
- известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;
- известить администратора безопасности ИСПДн о факте несанкционированного доступа.

- **ПРАВА**

Ответственный за организацию обработки персональных данных имеет право:

- Требовать от сотрудников выполнения локальных нормативно-правовых актов в части работы с персональными данными.
- Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.
- Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

- **ОТВЕТСТВЕННОСТЬ**

- Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.
- Ответственный за организацию обработки персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

С инструкцией ознакомлена:_____ /_____/