

Муниципальное дошкольное образовательное учреждение
«Рудновский детский сад»

ПРИНЯТО
Общим собранием
работников Учреждения

Протокол № 4 от 11.12.2022 г.



УТВЕРЖДАЮ
заведующий МДОУ
«Рудновский детский сад»
Л.А. Балакина
Приказ от 11.12.2022 г. №35

**Сведения о реализуемых требованиях
к защите персональных данных в муниципальном дошкольном
образовательном учреждении «Рудновский детский сад»**

В муниципальном дошкольном образовательном учреждении «Рудновский детский сад» (далее – Учреждение) приняты меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Реализуются следующие требования законодательства Российской Федерации в области персональных данных:

- требования о соблюдении конфиденциальности персональных данных;
- требования об обеспечении реализации субъектом персональных данных своих прав, включая право на доступ к информации;
- требования об обеспечении точности персональных данных, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных (с принятием (обеспечением принятия) мер по удалению или уточнению неполных или неточных данных);
- требования к защите персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- иные требования законодательства Российской Федерации.

Учреждение самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством в области персональных данных (ч.1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

В Учреждении в соответствии с действующим законодательством Российской Федерации разработан и введен в действие комплекс организационно-распорядительных и функциональных мер, регламентирующих и обеспечивающих безопасность обрабатываемых персональных данных:

- назначены ответственные лица за организацию и обеспечение безопасности персональных данных в Учреждении;

- введен режим безопасности обработки и обращения с персональными данными, а также режим защиты помещений, в которых осуществляется обработка и хранение носителей персональных данных;
- установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
- определен круг лиц, имеющих право обработки персональных данных, разработаны инструкции пользователям по защите персональных данных, антивирусной защите; - определены требования к персоналу, степень ответственности работников за обеспечение безопасности персональных данных;
- проведено ознакомление работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации по обеспечению безопасности персональных данных и требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, и другими локальными актами по вопросам обработки персональных данных;
- проводится периодическое обучение работников, осуществляющих обработку персональных данных, правилам обработки персональных данных;
- осуществляется контроль за соблюдением работниками, допущенных к обработке персональных данных, требований, установленных законодательством Российской Федерации в области персональных данных, локальными нормативными актами.
- Учреждение предпринимает необходимые и достаточные технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий:
- введена система разграничения доступа работников к информации, содержащей персональные данные субъектов персональных данных, в соответствии с их должностными (функциональными) обязанностями;
- установлена защита от несанкционированного доступа к рабочим местам и базам персональных данных;
- установлена антивирусная защита от вредоносного программного воздействия;
- осуществляется регулярное резервное копирование информации и баз данных, содержащих персональные данные субъектов персональных данных;
- передача персональных данных с использованием информационно-телекоммуникационных сетей осуществляется при помощи средств криптографической защиты информации (закрепляется электронной подписью руководителя);
- организован контроль за порядком обработки персональных данных и обеспечения их безопасности;
- проводятся регулярные внутренние проверки соответствия системы защиты персональных данных, аудит уровня защищенности персональных данных в информационных системах персональных данных, функционирования средств защиты информации, выявления изменений в режиме обработки и защиты персональных данных.