

Муниципальное бюджетное дошкольное образовательное учреждение  
детский сад общеразвивающего вида №13

**ПРИКАЗ**

от 11.01.2021 г.

№14

п.Комсомольский

**Об утверждении Перечень мер,  
направленных на исключение в МБДОУ д/с ОВ №13  
несанкционированного доступа и обеспечивающих сохранность  
персональных данных**

На основании Федерального закона от 27.07.2006 года №152-ФЗ  
«О персональных данных» и в соответствии с перечнем 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, утверждённым  
постановлением Правительства Российской Федерации от 21 марта 2012 года  
№211,

приказываю:

1. Утвердить Перечень мер, направленных на исключение в МБДОУ д/с  
ОВ №13 несанкционированного доступа и обеспечивающих  
сохранность персональных данных (приложение).
2. Контроль за исполнением настоящего приказа оставляю за собой.

Заведующий МБДОУ д/с ОВ №13



Л.И.Шостак

**Перечень мер,  
направленных на исключение в МБДОУ д/с ОВ №13  
несанкционированного доступа и обеспечивающих сохранность  
персональных данных**

## I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Перечень мер, направленных на исключение несанкционированного доступа и обеспечивающих сохранность персональных данных (далее - Перечень мер).

Муниципальное бюджетное дошкольное образовательное учреждение детский сад общеразвивающего вида №13 (далее-ДОУ) определяет порядок противодействия несанкционированному использованию персональных данных сотрудниками, имеющими доступ к такой информации, а также их ответственность, в случае совершения ими действий, повлекших неправомерное использование персональных данных.

1.2. Целью настоящего документа является установление в учреждении процедур, позволяющих:

- исключить возможность несанкционированного доступа к персональным данным и их использования работниками учреждения и третьими лицами в собственных интересах в ущерб интересам граждан;

## II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Перечне мер применяются следующие термины и определения:

2.1. Персональные данные (ПД) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.2. Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

2.3. Информационная система персональных данных - информационная система, представляющая собой совокупность

персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без наличия таких средств.

2.4. Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

2.5. Применяемые в Перечне мер понятия и определения, не приведенные в настоящем разделе, используются в соответствии с понятиями и определениями, содержащимися в законодательстве Российской Федерации.

### **III. ОБЩИЕ ПОЛОЖЕНИЕ О ПЕРСОНАЛЬНЫХ ДАННЫХ И ПОРЯДКЕ ИХ ИСПОЛЬЗОВАНИЯ**

3.1. Персональные данные могут быть представлены в различном виде, в том числе в бумажном или электронном.

3.2. Персональные данные могут передаваться только тем лицам, которым они необходимы для исполнения ими своих прямых должностных обязанностей.

3.3. Сотрудники ДОУ, осуществляющие проведение, обработку и учет персональных данных не имеют права передавать данную информацию третьим лицам и работникам ДОУ режим доступа которых не предусматривает возможности обладания такой информацией, либо использовать ее в личных целях.

3.4. За использование и разглашение персональных данных, сотрудник ДОУ несет персональную ответственность в соответствии с должностной инструкцией и действующим законодательством РФ.

### **IV. ОСНОВНЫЕ МЕРЫ (ПРОЦЕДУРЫ), ПРЕПЯТСТВУЮЩИЕ НЕСАНКЦИОНИРОВАННОМУ ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1. Под процедурами, препятствующими несанкционированному использованию персональных данных, в целях реализации настоящего документа, понимаются мероприятия по предупреждению несанкционированного использования, оперативному и последующему контролю использования персональных данных, проводимые сотрудниками ДОУ.

4.2. В ДОУ применяются следующие меры, препятствующие несанкционированному доступу к персональным данным:

- ограничение доступа к персональным данным в специализированных программных средствах;
- защита персональных данных при их обработке и архивировании;
- ограничение доступа посторонних лиц в помещения учреждения, предназначенные для осуществления работы с ПД;
- защита рабочих мест работников, осуществляющих операции с программными средствами;
- контроль за соблюдением работниками ДООУ требований законодательства РФ и иных нормативных правовых актов.

4.3. В целях противодействия несанкционированному использованию персональных данных, предотвращения утечки и обеспечения сохранности персональных данных, в ДООУ используется следующий комплекс мероприятий.

4.3.1. Ограничение доступа к служебной информации в программных средствах:

- обеспечение доступа к данным только в пределах полномочий, представленных непосредственно исполнителям, обеспечивающим ведение, обработку и учет информации с ПД;
- установление индивидуальных кодов и паролей доступа к данным для каждого исполнителя;
- осуществление административных и технических мер, направленных на исключение несанкционированного доступа к данным: блокирование доступа пользователя в систему, в случае обнаружения попыток несанкционированного доступа, установка программных средств, оповещающих ответственного за организацию работы по обеспечению защиты информации о попытке несанкционированного доступа, блокировка рабочего места нарушителя;
- контроль за соблюдением режима обращения персональных данных осуществляется ответственным за организацию работы по обеспечению защиты информации, а так же заведующим ДООУ.

4.3.2. Защита персональных данных при ее обработке и архивировании:

- обеспечение дублирования данных в процессе их ввода, предусматривающее сохранность первичного носителя информации;
- установка программных средств для создания резервных копии, способствующих быстрому восстановлению данных;
- использование систем защиты информационно-технических систем и каналов связи от утечки персональных данных;
- осуществление резервного копирования (восстановления) только уполномоченными сотрудниками:

4.3.3. Ограничение доступа посторонних лиц в помещении ДООУ, предназначенные для осуществления сбора, обработки и хранения информации ПД осуществляются за счёт:

- соблюдения порядка и правил доступа в служебные помещения в соответствии с Положением о защите ПД в ДОУ, утвержденным заведующим;
- ограничением доступа работников и посторонних лиц в помещение, в котором размещены персональные компьютеры, вычислительные системы и системы телекоммуникации для осуществления операций с ПД.

#### 4.3.1. Защита рабочих мест работников, осуществляющих сбор и обработку ПД:

- защита окон в служебных помещениях от внешнею дистанционного наблюдения жалюзи и шторами;
- эффективное размещение рабочих мест сотрудников для исключения возможности несанкционированного просмотра документов и информации на мониторах;
- соблюдение сотрудниками подразделений правил по обеспечению защиты информации при работе с персональными компьютерами.

#### 4.3.2. Ограничение доступа к персональным данным:

- доступ работников к необходимым документам, только для выполнения своих служебных обязанностей;
- проведение инвентаризации мест хранения документов, содержащих персональные данные;
- контроль за соблюдением утвержденных внутренних регламентов.

4.3.3. При оформлении на работу в ДОУ, работник дает расписку о неразглашении персональных данных.

4.3.4. Контроль за соблюдением работниками ДОУ требований законодательства РФ и иных нормативных правовых актов, регулирующих работу с ПД, внутренними документами, возложен на заведующего ДОУ.

### **III. ОСУЩЕСТВЛЕНИЕ ПРОЦЕДУР, ПРЕПЯТСТВУЮЩИХ НЕСАНКЦИОНИРОВАННОМУ ИСПОЛЬЗОВАНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ, И КОНТРОЛЯ ЗА ИХ ИСПОЛНЕНИЕМ**

5.1. Проведение процедур, препятствующих несанкционированному использованию персональных данных и осуществление контроля включают в себя:

5.1.1. Установление требований о неразглашении персональных данных.

5.1.2. Контроль за выполнением работниками ДОУ требований действующего законодательства РФ и внутренних документов ДОУ.

5.1.3. Уведомление работников ДОУ, имеющих доступ к информации о ПД, о недопустимости осуществления операций с ПД как в своих интересах, так и в интересах третьих лиц.

5.1.4. Проведение оперативных проверок на предмет возможной утечки персональных данных в случаях, предполагающих несанкционированное использование персональных данных.

5.1.5. Направление сведений руководству ДОУ об установленных (обнаруженных) случаях несанкционированного использования персональных данных.

#### **IV. ОТВЕТСТВЕННОСТЬ**

6.1 Ответственный за организацию работы по обеспечению защиты информации отвечает за:

- осуществление контроля исполнения положений нормативных документов по вопросам организации и эффективного функционирования системы внутреннего контроля ДОУ;
- контроль исполнения внутренних нормативных документов учреждения по вопросам обеспечения конфиденциальности персональных данных в ДОУ;
- проведение служебных расследований по фактам возможного неправомерного использования работниками ДОУ персональных данных, о результатах которых незамедлительно уведомляет заведующего.

6.2. Работники ДОУ, которым стали известны факты неправомерного использования персональных данных при осуществлении профессиональной деятельности, должны незамедлительно доложить об этом заведующему ДОУ.

6.3. Ответственность сотрудников и должностных лиц ДОУ за нарушения режима обращения с персональными данными и порядок наложения взыскания:

6.3.1. Виды взысканий, применяемых к сотрудникам и должностным лицам ДОУ нарушившим режим обращения с персональными данными:

- предупреждение;
- выговор;
- увольнение с работы;

6.3.2. Взыскание на сотрудника ДОУ налагается заведующим.

#### **V. МЕСТА РАЗДЕЛЬНОГО ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ**

7.1. Для исключения несанкционированного доступа к ПД в ДОУ приказом заведующего определяются места раздельного хранения персональных данных (материальных носителей) в отношении каждой категории персональных данных и устанавливается перечень лиц, осуществляющих обработку персональных данных.

Место хранения ПД	Наименование документов, содержащих ПД	Должность сотрудника, ответственного за хранение ПД
Кабинет заведующего, Сейф Шкаф металлический с замком	Информация о сотрудниках и обучающихся на электронных носителях Трудовые и медицинские книжки сотрудников ДОУ Личные дела, личные карточки Т-2, приказы по личному составу Личные дела обучающихся, алфавитная книга	Заведующий
Архив (отдельное помещение, под замком)	алфавитная книга	Заведующий
Кабинет заведующего,  Сейф Шкаф металлический с замком	Тарификация, Табель на зарплату	Заведующий
Кабинет заведующего,  Сейф Шкаф металлический с замком	Больничные листки. Приказы по личному составу	Заведующий
Медицинский Кабинет Шкаф металлический с замком	Медицинские карты обучающихся, работников	Старшая медицинская сестра

7.2. Ответственный за организацию работы по обеспечению защиты информации осуществляет ознакомление сотрудников ДОУ с настоящим Перечнем мер не позднее одного месяца со дня его вступления в силу. Факт ознакомления подтверждается подписью сотрудника. В дальнейшем, проводится регулярный инструктаж сотрудников с периодичностью не реже одного раза в год. с целью неукоснительного соблюдения сотрудниками мероприятий, направленных на предотвращение неправомерного использования персональных данных при осуществлении учреждения профессиональной деятельности.

7.3. Ответственный за организацию работы по обеспечению защиты информации, в случае принятия в штат ДОУ нового сотрудника, осуществляет ознакомление с настоящим Перечнем мер не позднее одной недели со дня его зачисления в штат.

7.4. Работники ДОУ должны предпринимать все необходимые меры, позволяющие предотвратить неправомерное распространение и использование персональных данных при проведении операции, связанных с осуществлением профессиональных видов деятельности.