Тыщенко Елена Михайловна

Подписан: Тыщенко Елена Михайловна
DN: ИНН=233705692230, СНИЛС=00580192522, E=buh-soh41@mail.ru, C=RU, S=Краснодарский край, L=станица Троицкая, O=МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД 13 СТАНИЦЫ ТРОИЦКОЙ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ КРЫМСКИЙ РАЙОН, G=Елена Михайловна, SN=Тыщенко, CN=Тыщенко Елена Михайловна
Основание: Я являюсь автором этого документа
Местоположение: станица Троицкая
Дата: 2021.08.10 15:48:56+03'00'

УТВЕРЖДАЮ
Заведующий
МБДОУ детского сада № 13
_____Е.М.Тыщенко
26.07.2021 г.

ПЕРЕЧЕНЬ МЕР, НАПРАВЛЕННЫХ НА ИСКЛЮЧЕНИЕ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И ОБЕСПЕЧИВАЮЩИХ СОХРАННОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Перечень мер, направленных на предотвращение неправомерного использования персональных данных (далее - Перечень мер) Муниципального бюджетного дошкольного образовательного учреждения детского сада № 13 станицы Троицкой муниципального образования Крымский район (далее – Учреждение) 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 Учреждения, осуществляющие проведение, обработку и учет персональных данных не имеют права передавать данную информацию третьим лицам и работникам Учреждени режим доступа которых не предусматривает возможности обладания такой информацией, либо использовать ее в личных целях.

3.4. За использование и разглашение персональных данных, сотрудник Учреждения 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 Учреждения.

4.2. В Учреждении 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 Учреждения 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 Учреждении 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 паролей доступа к данным;

- осуществление административных и технических мер, направленных на исключение несанкционированного доступа к данным;

- контроль за соблюдением режима обращения персональных данных осуществляется ответственным за организацию работы по обеспечению защиты информации, а так же заведующим Учреждения.

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 Учреждения, предназначенные для осуществления сбора, обработки и хранения информации ПД осуществляются за счѐт:

- соблюдения порядка и правил доступа в служебные помещения в соответствии с Положением о порядке обработки персональных данных субъектов Учреждения, утвержденном заведующим;

- ограничением доступа работников и посторонних лиц в помещение, в котором размешены персональные компьютеры.

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

- зашита 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.

4.3.5. 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.

4.3.6. При оформлении на работу в Учреждение, работник дает расписку о неразглашении персональных данных.

4.3.7. Контроль за соблюдением работниками Учреждения требований законодательства РФ и иных нормативных правовых актов, регулирующих работу с ПД возложен на заведующего Учреждения.

V. 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 Учреждения требований действующего законодательства РФ и внутренних документов Учреждения.
5.1.3. Уведомление работников Учреждения, 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 Учреждения об установленных (обнаруженных) случаях несанкционированного использования персональных данных.

VI. ОТВЕТСТВЕННОСТЬ

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

- осуществление контроля исполнения положений нормативных документов по вопросам организации и эффективного функционирования системы внутреннего контроля Учреждения;

- контроль исполнения внутренних нормативных документов учреждения по вопросам обеспечения конфиденциальности персональных данных в Учреждении:

- проведение служебных расследований по фактам возможною неправомерного использования работниками Учреждения персональных данных, о результатах которых незамедлительно уведомляет заведующего.

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

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

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

- предупреждение;

- выговор;

- увольнение с работы;

6.3.2. Взыскание на сотрудника Учреждения налагается заведующим.

VII. МЕСТА РАЗДЕЛЬНОГО ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Для исключения несанкционированного доступа к ПД в Учреждении 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
Методический кабинет, сейф	Информация о сотрудниках, обучающихся и их родителей (законных представителей), трудовые и медицинские книжки сотрудников ДОУ, личные дела, личные карточки Т-2, приказы по личному составу, личные дела обучающихся,	заведующий
Медицинский кабинет	Медицинские карты обучающихся	заведующий

7.2. Ответственный за организацию работы по обеспечению защиты информации осуществляет ознакомление сотрудников Учреждения 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.

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

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