Муниципальное бюджетное общеобразовательное учреждение «Андринская средняя общеобразовательная школа»
(МБОУ «Андринская СОШ»)

Федоренко Ольга Михайловна
Подписано цифровой подписью: Федоренко Ольга Михайловна
Дата: 2023.08.09 12:50:49 +05'00'

УТВЕРЖДАЮ
Директор МБОУ «Андринская СОШ»
_____О.М. Федоренко
(приказ от 07.08.2023г. № 469-од)

ПОЛОЖЕНИЕ
о защите персональных данных в МБОУ «Андринская СОШ»

1. Общие положения

1.1. Положение о защите персональных данных МБОУ «Андринская средняя общеобразовательная школа» (далее – Работодатель) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ и иными нормативно-правовыми актами в области защиты персональных данных, действующими на территории России.
1.2. Цель настоящего Положения – защита персональных данных работников МБОУ «Андринская СОШ» от несанкционированного доступа и разглашения, предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.
1.3. В целях настоящего Положения:

- под персональными данными (далее – ПД) понимается любая информация, прямо или косвенно относящаяся к субъекту персональных данных;
- под угрозами безопасности ПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных;
- под уровнем защищенности ПД понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности ПД при их обработке в информационной системе.

1.4. Настоящее Положение и изменения к нему утверждаются директором МБОУ «Андринская СОШ» и вводятся приказом. Все работники должны быть ознакомлены под подпись с данным Положением и изменениями к нему.
1.5. Настоящее Положение вступает в силу с 07.08.2023г.

2. Защита персональных данных

2.1. Работодатель принимает следующие меры по защите ПД:
2.1.1. Назначение лица, ответственного за обработку ПД, которое осуществляет организацию обработки ПД, обучение и инструктаж, внутренний контроль за соблюдением работниками требований к защите ПД.
2.1.2. Разработка политики в отношении обработки ПД.
2.1.3. Установление правил доступа к ПД, обеспечение регистрации и учета всех действий, совершаемых с ПД.
2.1.4. Установление индивидуальных паролей доступа сотрудников в информационную систему в соответствии с их производственными обязанностями.
2.1.5. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

2.1.6. Сертифицированное антивирусное программное обеспечение с регулярно обновляемыми базами.
2.1.7. Соблюдение условий, обеспечивающих сохранность ПД и исключающих несанкционированный к ним доступ.
2.1.8. Обнаружение фактов несанкционированного доступа к ПД.
2.1.9. Восстановление ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
2.1.10. Обучение работников, непосредственно осуществляющих обработку ПД, положениям законодательства РФ о персональных данных, в том числе требованиям к защите персональных данных, документам, определяющим политику Работодателя в отношении обработки ПД, локальным актам по вопросам обработки персональных данных.
2.1.11. Осуществление внутреннего контроля и аудита.
2.1.12. Определение типа угроз безопасности и уровней защищенности ПД, которые хранятся в информационных системах.
2.2. Угрозы защищенности персональных данных.
2.2.1. Угрозы первого типа. В системном программном обеспечении информационной системы есть функциональные возможности программного обеспечения, которые не указаны в описании к нему либо не отвечают характеристикам, которые заявил производитель. И это потенциально может привести к неправомерному использованию персональных данных.
2.2.2. Угрозы второго типа. Потенциальные проблемы с прикладным программным обеспечением — внешними программами, которые установлены на компьютерах работников.
2.2.3. Угрозы третьего типа. Потенциальной опасности ни от системного, ни от программного обеспечения нет.
2.3. Уровни защищенности персональных данных.
2.3.1. Первый уровень защищенности. Если работодатель отнес информационную систему к первому типу угрозы или если тип угрозы второй, но работодатель обрабатывает специальные категории ПД более 100 тыс. физических лиц без учета работников.
2.3.2. Второй уровень защищенности. Если тип угрозы второй и работодатель обрабатывает специальные категории ПД работников вне зависимости от их количества или специальные категории ПД менее чем 100 тыс. физических лиц, или любые другие категории ПД более чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории данных более чем 100 тыс. физических лиц.
2.3.3. Третий уровень защищенности. Если при втором типе угрозы работодатель обрабатывает общие ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает специальные категории ПД работников или менее чем 100 тыс. физических лиц, или при третьем типе угрозы работодатель обрабатывает биометрические ПД, или при третьем типе угрозы работодатель обрабатывает общие ПД более чем 100 тыс. физических лиц.
2.3.4. Четвертый уровень защищенности. Если при третьем типе угрозы работодатель обрабатывает только общие ПД работников или менее чем 100 тыс. физических лиц.
2.4. При четвертом уровне защищенности персональных данных работодатель:

- обеспечивает режим безопасности помещений, в которых размещаете информационную систему;
- обеспечивает сохранность носителей информации;
- утверждает перечень работников, допущенных до ПД;
- использует средства защиты информации, которые прошли оценку соответствия требованиям закона в области обеспечения безопасности информации.

2.5. При третьем уровне защищенности ПД дополнительно к мерам, перечисленным в пункте 2.4 настоящего Положения, работодатель назначает ответственного за обеспечение безопасности ПД в информационной системе.
2.6. При втором уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4, 2.5 настоящего Положения, работодатель ограничивает доступ к электронному журналу сообщений, за исключением работников, которым такие сведения необходимы для работы.
2.7. При первом уровне защищенности ПД дополнительно к мерам, перечисленным в пунктах 2.4—2.6 настоящего Положения, работодатель:

- обеспечивает автоматическую регистрацию в электронном журнале безопасности изменения полномочий работников по допуску к ПД в системе;
- создает отдел, ответственный за безопасность ПД в системе, либо возлагает такую обязанность на один из существующих отделов работодателя.

2.8. В целях защиты ПД на бумажных носителях работодатель:

- приказом назначает ответственного за обработку ПД;
- ограничивает допуск в помещения, где хранятся документы, которые содержат ПД работников;
- хранит документы, содержащие ПД работников в шкафах, запирающихся на ключ;
- хранит трудовые книжки работников в сейфе в отделе кадров.

2.9. В целях обеспечения конфиденциальности документы, содержащие ПД работников, оформляются, ведутся и хранятся только работниками отдела кадров, бухгалтерии и службы охраны труда работодателя.
2.10. Работники отдела кадров, бухгалтерии и службы охраны труда работодателя, допущенные к ПД работников, подписывают обязательства о неразглашении персональных данных. В противном случае до обработки ПД работников не допускаются.
2.11. Допуск к документам, содержащим ПД работников, внутри организации осуществляется на основании Регламента допуска работников к обработке персональных данных.
2.12. Передача ПД по запросам третьих лиц, если такая передача прямо не предусмотрена законодательством РФ, допускается исключительно с согласия работника на обработку его персональных данных в части их предоставления или согласия на распространение персональных данных.
2.13. Передача информации, содержащей сведения о ПД работников, по телефону в связи с невозможностью идентификации лица, запрашивающего информацию, запрещается.
2.14. Определение уровня защищенности персональных данных при их обработке в информационных систем персональных данных Школы, осуществляется в порядке, установленном законодательством Российской Федерации.
2.15. Работникам Школы, имеющим право осуществлять обработку персональных данных в информационных системах Школы, предоставляется уникальный логин и пароль для доступа к соответствующей информационной системе Школы. Доступ предоставляется к прикладным программным подсистемам в соответствии с функциями, предусмотренными должностными обязанностями работников. Информация вносится в ручном режиме, при получении информации на бумажном носителе или в ином виде, не позволяющем осуществлять ее автоматическую регистрацию.
2.16. Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных Школы, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по обеспечению безопасности:
2.16.1. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

2.16.2. Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных.
2.16.3. Применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации.
2.16.4. Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных.
2.16.5. Учет машинных носителей персональных данных.
2.16.6. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.
2.16.7. Восстановление персональных данных, модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.
2.16.8. Установление правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных Школы, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных.
2.16.9. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровней защищенности информационных систем персональных данных.
2.17.Инженер ЭВМ Школы, ответственный за обеспечение информационной безопасности, организует и контролирует ведение учета материальных носителей персональных данных и обеспечивает:
2.17.1. Своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в Школе.
2.17.2. Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование. 2.17.3. Возможность восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
2.17.4. Постоянный контроль за обеспечением уровня защищенности персональных данных. 2.17.5. Знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
2.17.6. Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.
2.17.7. При обнаружении нарушений порядка представления персональных данных незамедлительное приостановление представления персональных данных пользователям информационной системы персональных данных до выявления причин нарушений и устранения этих причин.
2.17.8. Разбирательство и составление заключений по фактам несоблюдения условий хранения материальных носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
2.18. Ответственными за выполнение требований по защите персональных данных при их обработке в информационных системах персональных данных являются руководители структурных подразделений Школы (иные лица назначенные приказом), эксплуатирующих, а также использующих информационные системы, пользователи информационных систем, администратор безопасности. Администратор безопасности принимает все необходимые меры по восстановлению персональных данных,

модифицированных или удаленных, уничтоженных вследствие несанкционированного доступа к ним.
2.19. Обмен персональными данными при их обработке в информационных системах персональных данных Школы осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения сертифицированных программных и технических средств.
2.20. Доступ работников, допущенных к обработке персональных данных, предусматривает обязательное прохождение процедуры идентификации и аутентификации пользователя.
2.21. В случае выявления нарушений порядка обработки персональных данных в информационных системах персональных данных Школы уполномоченными должностными лицами незамедлительно принимаются меры по установлению причин нарушений и их устранению.

3. Гарантии конфиденциальности персональных данных

3.1. Все работники организации, осуществляющие обработку ПД, обязаны хранить тайну о сведениях, содержащих ПД, в соответствии с Положением, требованиями законодательства РФ.
3.2. Работник вправе требовать полную информацию о своих персональных данных, об их обработке, использовании и хранении.
3.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПД работников, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством.