СЕВЕРО-КАВКАЗСКИЙ
МЕДИЦИНСКИЙ
КОЛЛЕДЖ

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКИЙ МЕДИЦИНСКИЙ КОЛЛЕДЖ»

УТВЕРЖДАЮ
Директор АНО СПО "СКМК"

ДОКУМЕНТ ПОДПИСАН
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат:
0128CABE0060B0A5AD4494AF47B1C7615F
Владелец: Станислав Сергеевич Наумов
Действителен с 16.08.2023 до 16.11.2024

Приказ от 27.05.2024 № 30/2-ОД
03 июня 2024 г.

ПРАВИЛА
осуществления внутреннего контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требований к защите персональных данных

1. Правила осуществления внутреннего контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требований к защите персональных данных (далее – Правила) автономной некоммерческой организации среднего профессионального образования "Северо-Кавказский медицинский колледж" (далее – АНО СПО "СКМК") разработаны и утверждены в соответствии со следующими нормативными правовыми актами:

– Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (Собрание законодательства Российской Федерации, № 31, 31.07.2006, ст. 3448);

– Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701);

– Перечень сведений конфиденциального характера, утвержден Указом Президента Российской Федерации от 06.03.1997 г. № 188 (Собрание законодательства Российской Федерации, № 10, 10.03.97, ст. 1127);

– Требования к защите персональных данных при их обработке в информационных системах персональных данных, утверждены постановлением Правительства Российской Федерации от 01.11.2012 № 1119 (Собрание законодательства Российской Федерации, № 45, 05.11.2012, ст. 6257);

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержден приказом ФСТЭК России от 18.02.2013 № 21 (Зарегистрировано в Министерстве юстиции Российской Федерации 14.05.2013, регистрационный № 28375);

– Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утверждено постановлением Правительства Российской Федерации от 15.09.2008 № 687 (Собрание законодательства Российской Федерации, № 38, 22.09.2008, ст. 4320);

– Для служебного пользования;

– Методический документ "Меры защиты информации в государственных информационных системах", утвержден ФСТЭК России 11.02.2014.

2. Настоящими Правилами определяются процедура, направленная на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок и формы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в АНО СПО "СКМК".

3. В целях осуществления внутреннего контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требований к защите персональных данных, в АНО СПО "СКМК" организуется проведение плановых и внеплановых проверок условий обработки персональных данных на предмет соответствия Федеральному закону от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2011, № 31, ст. 4701) и принятым в соответствии с ним нормативным правовым актам, внутренним организационно-распорядительным документам АНО СПО "СКМК".

4. Внутренний контроль и аудит соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, осуществляется постоянно действующей комиссией (далее – Комиссия).

5. Комиссия состоит из председателя Комиссии, ответственного секретаря Комиссии и членов Комиссии.

6. Председателем Комиссии выступает ответственный за организацию обработки персональных данных в АНО СПО "СКМК", который вносит предложения директору АНО СПО "СКМК" по составу Комиссии и осуществляет руководство деятельностью Комиссии.

Персональный состав комиссии устанавливается приказом директора АНО СПО "СКМК".

7. Председатель Комиссии:

– является председательствующим на заседании Комиссии;

– осуществляет общее руководство и планирование деятельности Комиссии;

– принимает решение о проведении заседания Комиссии;

– определяет дату, место и время заседания Комиссии;

– утверждает повестку заседаний Комиссии, проводит заседания Комиссии;

– подписывает протокол заседания Комиссии;

– координирует работу членов Комиссии;

– распределяет между членами Комиссии вопросы для подготовки к заседаниям Комиссии;

– контролирует исполнение принятых на заседании решений Комиссии.

– дает поручения ответственному секретарю и членам Комиссии.

8. Ответственный секретарь Комиссии:

– осуществляет подготовку и организует проведение заседания Комиссии;

– своевременно уведомляет членов Комиссии, заинтересованные органы и организации о месте, дате, времени проведения заседания Комиссии;

– координирует деятельность членов Комиссии;

– готовит проекты повесток заседаний Комиссии и представляет на утверждение председателю Комиссии;

– совместно с членами Комиссии готовит информацию, документы, иные материалы к заседаниям Комиссии;

– ведет протокол заседания Комиссии;

– подписывает протокол заседания Комиссии, копии и выписки из него;

– обеспечивает организацию делопроизводства и хранение документов и материалов заседаний Комиссии

– осуществляет иные функции по обеспечению деятельности Комиссии.

9. Члены Комиссии:

– лично участвуют в заседании Комиссии;

– подготавливают материалы для заседаний Комиссии и предоставляют их ответственному секретарю Комиссии;

– формируют запросы о получении информации, необходимой для работы Комиссии;

– знакомятся с информацией, документами и материалами по вопросам, вынесенным на обсуждение Комиссии;

– участвуют в обсуждении вопросов, включенных в повестку заседания Комиссии;

– подготавливают проекты решений и рекомендаций по рассматриваемым вопросам;

– в случае несогласия с принятым решением излагают свое особое мнение в письменном виде, которое вносится в протокол заседания Комиссии.

10. Каждый член Комиссии имеет право вносить свои предложения по любым вопросам работы Комиссии.

11. Заседание Комиссии считается правомочным, если на нем присутствует более 70 % членов Комиссии.

12. Решения Комиссии принимаются простым большинством голосов членов Комиссии в ходе открытого голосования.

Каждый член Комиссии, включая ответственного секретаря Комиссии, имеет один голос. При равенстве голосов принятым считается решение, за которое проголосовал председательствующий на заседании Комиссии.

13. Особое мнение членов Комиссии, голосовавших против принятого решения, излагается в письменном виде и отражается в протоколе заседания Комиссии.

14. Заседания Комиссии проводятся по мере необходимости.

15. Решение Комиссии оформляется актом (протоколом).

Акт (протокол) внутреннего контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, должен содержать сведения о выявленном нарушении (содержание нарушения) и сроке его устранения.

16. Акт (протокол) подписывается Комиссией и утверждается директором АНО СПО "СКМК".

Утвержденный акт (протокол) доводится до сведения проверяемого лица под роспись. Экземпляр утвержденного акта (протокола) выдается проверяемому лицу под роспись.

17. Внесение изменений в состав Комиссии допускается на основании мотивированной служебной записки председателя Комиссии.

18. Ответственный секретарь Комиссии в течение 3 (трех) рабочих дней после согласования служебной записки подготавливает проект приказа о внесении изменений в состав Комиссии.

19. Прием-передача документов и иных материалов по результатам работы Комиссии оформляется актом в установленном порядке.

20. Комиссия подлежит расформированию в следующих случаях:

а) вывод из эксплуатации информационных (автоматизированных) систем АНО СПО "СКМК", прекращение обработки конфиденциальной информации, в том числе содержащей персональные данные;

б) ликвидация, реорганизация АНО СПО "СКМК" и (или) изменение его организационно-правовой формы, в результате которых были утрачены признаки оператора персональных данных.

21. Комиссия имеет право:

1) Участвовать в работе органов управления АНО СПО "СКМК" и в рассмотрении вопросов, предусмотренных задачами и функциями Комиссии;

2) Получать от структурных подразделений и работников АНО СПО "СКМК" необходимые для деятельности Комиссии документы и иную служебную информацию;

3) Вносить предложения по совершенствованию деятельности Комиссии;

4) Требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;

5) Принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

6) Вносить директору АНО СПО "СКМК" предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

7) Вносить директору АНО СПО "СКМК" предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных;

8) Совершать в рамках закона иные действия, соответствующие задачам и функциям Комиссии.

22. Внутренний контроль и аудит соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, осуществляется на основании ежегодного плана проверок (плановые проверки) не реже одного раза в год, а также по решению председателя Комиссии (внеплановые проверки).

23. План внутреннего контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, разрабатывается Комиссией и утверждается директором АНО СПО "СКМК".

В плане по каждой проверке устанавливаются объект и предмет проверки, проверяемый период, срок ее проведения и ответственный исполнитель.

24. План внутреннего контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, подлежит обязательному опубликованию на официальном сайте АНО СПО "СКМК" (skmk-stav.ru) в течение 10 календарных дней с даты утверждения.

25. В случае выявления нарушения требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, председатель Комиссии инициирует проведение повторной проверки в течение

10 календарных дней с даты истечения срока его устранения, указанного в акте (протоколе).

26. Председатель Комиссии вправе инициировать проведение внепланового контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, при наличии следующих оснований:

1) Требование контрольного (надзорного) органа, в том числе уполномоченного органа по защите прав субъектов персональных данных;

2) Письменное заявление (служебная записка) о нарушениях правил обработки персональных данных;

3) Зарегистрированная в установленном порядке нештатная ситуация, компьютерный инцидент, компьютерная атака на информационные системы персональных данных, требующая проведения расследования;

4) Иные признаки нарушения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, внутренних организационно-распорядительных документов АНО СПО "СКМК" в области защиты персональных данных, выявленные председателем, ответственным секретарем, членами Комиссии, уполномоченными должностными лицами отдела цифрового развития и информационной безопасности, отдела комплексной безопасности.

27. Проведение внепланового контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, организуется в течение 3 рабочих дней с момента появления соответствующих оснований.

28. При проведении контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, должны быть полностью, объективно и всесторонне определены:

1) Порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

2) Порядок и условия применения средств защиты информации;

3) Эффективность принимаемых мер по обеспечению безопасности персональных данных в ходе эксплуатации информационной системы персональных данных;

4) Состояние учета машинных носителей персональных данных;

5) Соблюдение правил доступа к персональным данным;

6) Наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

7) Мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) Осуществление мероприятий по обеспечению целостности персональных данных.

29. В отношении персональных данных, ставших известными председателю, ответственному секретарю, членам Комиссии в ходе проведения внутреннего контроля и аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, должна обеспечиваться конфиденциальность.

30. Внутренний контроль аудит соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе

требованиям к защите персональных данных должен быть завершена не позднее чем через десять дней со дня принятия решения о ее проведении.

31. Контроль за своевременностью и правильностью проведения внутреннего контроля аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, в том числе требованиям к защите персональных данных, возлагается на председателя Комиссии.

Начальник отдела цифрового развития и информационной безопасности

ДОКУМЕНТ ПОДПИСАН УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 01DAB0D0459093C000193FF410EF0001
Владелец: Сергей Викторович Семенов
Действителен с 28.05.2024 до 28.05.2025

С. В. Семенов

03 июня 2024 г.