Приложение №1 к Приказу № 194 от 31.08.18.

ПОЛОЖЕНИЕ

О КОМИССИИ ПО ПРИВЕДЕНИЮ В СООТВЕТСТВИЕ С ТРЕБОВАНИЯМИ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Кемерово, Кемеровская область, 2018 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о комиссии по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Положение) определяет основные задачи, функции и права комиссии, в обязанности которой входит проведение работ по обеспечению безопасности и организации обработки персональных данных в муниципальное бюджетное общеобразовательное учреждение "Средняя общеобразовательная школа №49" (далее – Оператор).

1.2. Комиссия по приведению Оператора в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Комиссия), назначается на весь период обработки персональных данных у Оператора приказом руководства Оператора.

1.3. В состав Комиссии добавляются новые члены приказом руководства Оператора.

1.4. Из состава Комиссии сотрудники исключается на основании приказа руководства Оператора.

1.5. Основной задачей Комиссии является приведение деятельности Оператора в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее – Требования) и контроль над исполнением основных положений законодательства.

1.6. Свою деятельность Комиссия осуществляет в соответствии с «Планом мероприятий по приведению муниципальное бюджетное общеобразовательное учреждение "Средняя общеобразовательная школа №49" в соответствие с требованиями законодательства Российской Федерации в области персональных данных», утверждаемым руководством Оператора.

1.7. Комиссия самостоятельно разрабатывает «План мероприятий по приведению муниципальное бюджетное общеобразовательное учреждение "Средняя общеобразовательная школа №49" в соответствие с требованиями законодательства Российской Федерации в области персональных данных» и передает руководству Оператора на утверждение.

1.8. В своей деятельности Комиссия руководствуется законодательными и нормативно-правовыми актами Российской Федерации в области персональных данных, настоящим Положением и иными нормативными актами Оператора.

1.9. Законодательные и нормативно-правовые акты Российской Федерации в области персональных данных приведены в Приложении №1 к настоящему Положению.

2. ОРГАНИЗАЦИОННАЯ СТРУКТУРА КОМИССИИ

2.1. Комиссия состоит из Председателя Комиссии и членов Комиссии.

2.2. Комиссия возглавляется Председателем Комиссии.

2.3. Комиссия подчиняется руководству Оператора.

2.4. Из состава Комиссии назначается лицо, ответственное за организацию обработки персональных данных, и администратор безопасности информационных систем персональных данных.

3. ОСНОВНЫЕ ФУНКЦИИ КОМИССИИ

3.1. Разработка проектов документов, необходимых для выполнения Требования законодательства и представленных в Приложении №2 к настоящему Положению.

3.2. Организация и проведение работ по обеспечению безопасности помещений, в которых производится обработка персональных данных, а также находятся на хранении материальные носители персональных данных.

3.3. Анализ и оценка соответствия внутренних нормативных документов Оператора, в части касающейся обработки персональных данных, а в случае выявления несоответствий – внесение необходимых изменений.

3.4. Организация и проведение работ по обучению и повышению осведомленности персонала в области персональных данных.

3.5. Анализ изменений законодательства Российской Федерации в области персональных данных.

3.6. Оценка выполнения Оператором обязанностей, установленных законодательством Российской Федерации в области персональных данных, а в случае выявления несоответствий – выработка рекомендаций по их устранению.

3.7. Организация подготовки и направления в уполномоченный орган по защите прав субъектов персональных данных Уведомления об обработке персональных данных, а в случае изменения сведений, содержащихся в Реестре операторов, осуществляющих обработку персональных данных, направление сведений о таких изменениях.

3.8. В случае выявления неправомерных действий с персональными данными, Комиссия направляет уведомление об устранении нарушений.

3.9. Анализ и оценка соответствия Требованиям законодательства типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, а в случае выявления несоответствий – выработка рекомендаций по их устранению.

3.10. Анализ и оценка соответствия договорной базы Оператора Требованиям законодательства, а в случае выявления несоответствий – внесение соответствующих изменений и дополнений.

3.11. Контроль выполнения Требований законодательства, в части касающейся согласия субъектов персональных данных на обработку их персональных данных.

3.12. Общий контроль соблюдения Оператором требований по обеспечению безопасности персональных данных и соблюдения Требований законодательства.

3.13. Организация работ и сбор необходимых документов при прохождении федерального государственного контроля (надзора) за соответствием обработки персональных данных Требованиями законодательства.

3.14. Ведение журнала по учету проверок в соответствии с Требованиями законодательства.

3.15. Организация работ по разработке моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных Оператора, в том числе:

3.15.1. оценка полноты и правильности определения угроз безопасности;

3.15.2. плановый и внеплановый пересмотр.

3.16. Организация работ по созданию системы защиты персональных данных (комплекса организационно-технических мер), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности информационных систем персональных данных.

3.17. Проверка готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации.

3.18. Обучение лиц, применяющих средства защиты информации, правилам работы с ними.

3.19. Организация учета применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

3.20. Контроль выполнения мероприятий по защите персональных данных, реализуемых в рамках подсистем защиты с учетом уровня защищенности информационной системы персональных данных (не реже 1 раза в 3 года):

3.20.1. идентификация и аутентификация субъектов доступа и объектов доступа;

3.20.2. управление доступом субъектов доступа к объектам доступа;

3.20.3. ограничение программной среды;

3.20.4. защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);

3.20.5. регистрация событий безопасности;

3.20.6. антивирусная защита;

3.20.7. обнаружение (предотвращение) вторжений;

3.20.8. контроль (анализ) защищенности персональных данных;

3.20.9. обеспечение целостности информационной системы и персональных данных;

3.20.10. обеспечение доступности персональных данных;

3.20.11. защита среды виртуализации;

3.20.12. защита технических средств;

3.20.13. защита информационной системы, ее средств, систем связи и передачи данных;

3.20.14. выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;

3.20.15. управление конфигурацией информационной системы и системы защиты персональных данных.

3.21. Контроль за соответствием условий эксплуатации информационных систем персональных данных требованиям организационно-технической и эксплуатационной документации.

3.22. Контроль соблюдения работниками Оператора установленных требований по обеспечению безопасности персональных данных, проведение разбирательств и составление заключений по фактам несоблюдения данных требований.

3.23. Проведение внутренних проверок состояния защиты персональных данных.

3.24. Анализ эффективности и достаточности принятых мер и применяемых средств защиты персональных данных.

3.25. Разработка предложений по совершенствованию системы защиты персональных данных.

3.26. Решение вопросов, связанных с обслуживанием и эксплуатацией информационных систем:

3.26.1. эксплуатация информационных систем персональных данных в соответствии с организационно-технической и эксплуатационной документацией;

3.26.2. обеспечение работоспособности системы защиты персональных данных, реализуемой в рамках подсистем защиты с учетом уровня защищенности информационной системы;

3.26.3. организация мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

3.26.4. организация учета и использования машинных носителей информации;

3.26.5. организация работ по привлечению сторонних организаций для формирования и сопровождения баз данных и информационного взаимодействия (центров обработки информации), выполняющих функции операторов и администраторов системы централизованной обработки данных;

3.26.6. установка и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

3.26.7. учет лиц, допущенных к работе с персональными данными в информационных системах персональных данных.

3.27. Организация работ по размещению оборудования информационных систем персональных данных в части выполнения требований по сохранности носителей персональных данных и средств защиты информации, а также исключения возможности проникновения и неконтролируемого пребывания посторонних лиц на охраняемую территорию.

3.28. Уточнение персональных данных субъектов.

3.29. Блокирование обработки персональных данных субъектов.

3.30. Уничтожение персональных данных (по достижении целей обработки или в случае утраты необходимости в их достижении) при их автоматизированной обработке.

3.31. Обеспечение безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации.

3.32. Организация работ по ознакомлению работников Оператора, осуществляющих обработку персональных данных без использования средств автоматизации, а также лиц, осуществляющих такую обработку по договору с Оператором, о факте обработки ими персональных данных без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

3.33. Обеспечение раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.34. Организация работ по уничтожению материальных носителей персональных данных в случае достижения целей обработки или в случае утраты необходимости в их достижении с составлением актов об уничтожении.

3.35. Контроль выполнения требований настоящего Положения.

3.36. Определение уровня защищенности информационных систем персональных данных.

4. ПРАВА КОМИССИИ

4.1. Запрос и получение необходимых материалов для организации и проведения работ по вопросам обеспечения безопасности персональных данных у Оператора.

4.2. Привлечение к проведению работ по защите персональных данных на договорной основе сторонних организаций.

4.3. Контроль деятельности структурных подразделений Оператора в части выполнения ими требований по обеспечению безопасности персональных данных.

4.4. Внесение предложений руководству Оператора о приостановке работ в случае обнаружения несанкционированного доступа, утечки персональных данных, а также в случае предпосылок нарушения безопасности персональных данных.

5. ОТВЕТСТВЕННОСТЬ

5.1. Председатель Комиссии и члены Комиссии несут ответственность в соответствии с законодательством Российской Федерации.

С ПОЛОЖЕНИЕМ ОЗНАКОМЛЕНЫ:

Заместитель директора по БЖ	_____	Морозкина Н.И.
заместитель директора по АХР	_____	Яковлева О.В.
председатель ПК	_____	Голубина И.В.

ПРИЛОЖЕНИЕ №1

Законодательные и нормативно-правовые акты Российской Федерации в области персональных данных

Законодательные акты:

- Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 21 июля 2014 года N 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях».

Указы и Распоряжения Президента Российской Федерации:

- Указ Президента Российской Федерации от 30 мая 2005 года N 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;
- Указ Президента Российской Федерации от 6 марта 1997 года N 188 «Об утверждении перечня сведений конфиденциального характера».

Постановления Правительства Российской Федерации:

- Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 21 марта 2012 г. N 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных"»
- Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановление Правительства РФ от 6 июля 2008 г. N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

Нормативные правовые акты федеральных органов исполнительной власти:

- Приказ ФСБ РФ от 10.07.2014 № 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";

- ФСТЭК Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- ФСТЭК Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных при их обработке в информационных системах персональных данных;

- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ Минкомсвязи РФ от 28.08.2015 № 315 "О внесении изменений в Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по предоставлению государственной услуги "Ведение реестра операторов, осуществляющих обработку персональных данных", утвержденный приказом Министерства связи и массовых коммуникаций Российской Федерации от 21.12.2011 № 346";

- Приказ Министерства связи и массовых коммуникаций Российской Федерации от 14 ноября 2011 г. N 312 «Об утверждении Административного регламента исполнения Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций государственной функции по осуществлению государственного

контроля (надзора) за соответствием обработки персональных данных требованиям законодательства российской федерации в области персональных данных».

ПРИЛОЖЕНИЕ №2

Документы, необходимые для выполнения требований законодательства Российской Федерации в области персональных данных

№	ДОКУМЕНТ
1.	Положение о комиссии по приведению муниципальное бюджетное общеобразовательное учреждение "Средняя общеобразовательная школа №49" в соответствие с требованиями законодательства Российской Федерации в области персональных данных
2.	План мероприятий по приведению муниципальное бюджетное общеобразовательное учреждение "Средняя общеобразовательная школа №49" в соответствие с требованиями законодательства в области персональных данных
3.	Приказ об утверждении перечней
4.	Перечень должностей и третьих лиц, имеющих доступ к персональным данным
5.	Форма Обязательства о неразглашении персональных данных
6.	Форма Соглашения об обеспечении безопасности персональных данных, переданных на обработку
7.	Перечень обрабатываемых персональных данных
8.	Форма Согласия на обработку персональных данных
9.	Перечень информационных систем персональных данных
10.	Перечень применяемых средств защиты информации
11.	Технический паспорт информационных систем персональных данных
12.	Перечень помещений для обработки персональных данных
13.	Приказ о назначении лиц, ответственных за обработку и защиту персональных данных
14.	Инструкция администратора безопасности информационных систем персональных данных
15.	Инструкция лица, ответственного за организацию обработки персональных данных
16.	Положение по обработке персональных данных
17.	Политика оператора в отношении обработки персональных данных
18.	Положение об обеспечении безопасности персональных данных
19.	Регламент определения уровней защищенности персональных данных,

	обрабатываемых в информационных системах персональных данных
20.	Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных
21.	Протокол определения ущерба субъекту персональных данных
22.	Акт определения уровня защищенности информационных систем персональных данных
23.	Техническое задание на систему защиты персональных данных
24.	Уведомление об обработке персональных данных
25.	Приказ об утверждении Инструкции пользователя информационных систем персональных данных
26.	Инструкция пользователя информационных систем персональных данных
27.	Регламент по учёту, хранению и уничтожению носителей персональных данных
28.	Регламент по допуску сотрудников и третьих лиц к обработке персональных данных
29.	Регламент по реагированию на запросы субъектов персональных данных
30.	Регламент по взаимодействию с органами государственной власти в области персональных данных
31.	Регламент по резервному копированию персональных данных
32.	Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности
33.	Регламент по обезличиванию персональных данных
34.	Регламент по трансграничной передаче персональных данных