УПРАВЛЕНИЕ ОБРАЗОВАНИЯ
администрации Старооскольского
городского округа Белгородской области

ПРИКАЗ

« 23 » июня 2021 года № 899

Об утверждении Порядка осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации в сфере защиты персональных данных

В целях реализации Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», распоряжением Губернатора Белгородской области от 08 июня 2021 года № 265-р «О реализации Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

п р и к а з ы в а ю :

1. Утвердить Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации в сфере защиты персональных данных (прилагается).
2. Настоящий приказ вступает в силу со дня его подписания.
3. Контроль за исполнением приказа оставляю за собой.

Начальник управления образования администрации Старооскольского городского округа **Н.Е. Дереча**

Жигачёв Андрей Владимирович, (4725) 22-64-21

Приложение 1
к приказу управления образования
Старооскольского городского округа
№ _____ от «___» _____ 2021 г.

Порядок
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации в сфере защиты персональных данных

1. Настоящий порядок определяет основания, структуру, формы и методы проведения внутреннего контроля соответствия обработки персональных данных в управлении образования администрации Старооскольского городского округа Белгородской области (далее - управление образования).

2. В целях осуществления внутреннего контроля проводятся мероприятия по мониторингу соблюдения условий обработки и защиты персональных данных (далее — мероприятия внутреннего контроля).

3. Внутренний контроль проводится комиссией, создаваемой приказом управления образования (далее - Комиссия).

4. В состав Комиссии входят работники управления образования, могут привлекаться внешние эксперты.

5. В проведении внутреннего контроля не могут участвовать сотрудники управления образования, прямо или косвенно заинтересованные в его результатах.

6. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных — субъектов персональных данных.

7. Комиссия для реализации своих полномочий имеет право:

- привлекать к проведению проверок сотрудников управления образования;
- запрашивать информацию у сотрудников управления образования;
- принимать меры по устранению выявленных нарушений;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в сфере персональных данных.

8. Целями осуществления внутреннего контроля являются:

-оценка выполнения в управлении образования требований по обработке и защите персональных данных, установленных законодательством Российской Федерации;

-выявление и предотвращение в управлении образования нарушений законодательства Российской Федерации в сфере персональных данных.

9. Внутренний контроль осуществляется в управлении образования путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов по обработке и защите персональных данных.

10. Проверки соблюдения требований законодательства в сфере персональных данных и внутренних документов по обработке и защите персональных данных в управлении образования разделяются:

- на плановые;
- на внеплановые.

11. Внутренний контроль проводится не реже двух раз в год в соответствии с Планом проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - План внутреннего контроля).

Форма Плана внутреннего контроля определяется управлением образования самостоятельно. План внутреннего контроля разрабатывается и утверждается ежегодно.

12. Мероприятия по внутреннему контролю делятся на два основных этапа:

- проверяется порядок и условия применения организационных мер, необходимых для выполнения требований к защите персональных данных, в том числе проводится проверка наличия и актуальности документов;
- проверяется порядок и условия применения технических мер, необходимых для выполнения требований к защите персональных данных.

13. Перечень мероприятий, осуществляемых в ходе внутреннего контроля:

- осуществление проверки выполнения мер, а также наличия и актуальности документов, разработанных в соответствии с требованиями постановления Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня 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»;
- проверка соответствия установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей сотрудников управления образования;
- проверка подтверждения факта ознакомления — ответственных должностных лиц за организацию обработки персональных данных в управлении образования, должностных лиц, непосредственно осуществляющих обработку персональных данных в управлении образования, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, и правовыми актами по вопросам обработки персональных данных при их назначении на должность в управлении образования;
- проверка соответствия целей обработки содержанию и объему обрабатываемых персональных данных;
- выборочные проверки уровня знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных ответственных должностных лиц за организацию обработки персональных данных в управлении образования, должностных лиц, непосредственно осуществляющих обработку персональных данных в управлении образования;
- контроль соблюдения сроков хранения и порядка уничтожения носителей персональных данных;
- проверка соблюдения процедур и сроков подготовки ответов на обращения субъектов персональных данных в соответствии со статьями 20 и 21 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- проверка наличия и (или) необходимости актуализации уведомления об обработке персональных данных;

- проверка соблюдения условий эксплуатации средств защиты информации, используемых для обеспечения защиты персональных данных, входящих в зону ответственности управления образования, предусмотренных эксплуатационной и технической документацией на них;

- проверка функционирования технических средств защиты информации, используемых при обеспечении защиты персональных данных, входящих в зону ответственности управления образования;

- проверка выполнения мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее — ИСПДн). Включает в себя контрольные мероприятия по аудиту:

функционирования в штатном режиме средств антивирусной защиты, в том числе регулярности обновления антивирусных баз;

выполнения мер защиты при проведении резервного копирования программных средств, архивов, журналов, информационных активов, используемых и создаваемых в процессе эксплуатации ИСПДн;

наличия установленных обновлений безопасности программного обеспечения, в том числе программного обеспечения средств защиты информации;

регистрации событий информационной безопасности;

выполнения требований к системе защиты персональных данных в ИСИДн;

- проверка правильности эксплуатации средств криптографической защиты информации при их использовании в управлении образования;

- выполнение организационных и технических мероприятий по обеспечению пропускного режима в управлении образования.

Перечень и содержание проверок может корректироваться исходя из специфики деятельности управления образования.

14. Мероприятия внутреннего контроля осуществляются:

- путем опроса либо при необходимости путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных;

- путем анализа документов, регламентирующих обработку и защиту персональных данных;

- путем проведения при необходимости инструментальных проверок защищенности информационных систем персональных данных.

15. По результатам мероприятий внутреннего контроля Комиссией составляется протокол проведения внутреннего контроля (далее — Протокол), в котором будет отражена информация по рассмотренным вопросам, выявленные недостатки (при наличии), а также рекомендации по их устранению.

Протокол составляется не позднее 10 (десяти) календарных дней со дня окончания срока проведения мероприятия внутреннего контроля, подписывается всеми членами Комиссии.

16. В целях контроля устранения выявленных нарушений Комиссия может проводить повторные проверки.

17. По решению председателя Комиссии может быть проведено дополнительное мероприятие внутреннего контроля (внеплановая проверка) по следующим основаниям:

- окончание рекомендованного срока устранения выявленных в ходе мероприятий внутреннего контроля недостатков;

- результаты расследования выявленных нарушений требований законодательства в сфере персональных данных;

- результаты внешних контрольных мероприятий, проводимых уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных;

- существенные изменения процессов или процедур обработки и защиты персональных данных;

- выявленные значительные нарушения требований законодательства в сфере персональных данных или повторяемость нарушений;

- указание руководителя органа власти Белгородской области.

18. Решение о проведении дополнительного мероприятия внутреннего контроля принимается не позднее 30 (тридцати) календарных дней со дня наступления обстоятельств, указанных в пункте 17 настоящего типового порядка.