

Утверждаю
приказ КОГОАУ «КЭПЛ»
от 03.09.2021 г. № 83/З
директор _____ Н.А.Чернышева

ИНСТРУКЦИЯ
лица, ответственного за организацию обработки, обеспечение информационной безопасности персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки, обеспечение информационной безопасности персональных данных в КОГОАУ «Кировский экономико-правовой лицей», далее – Организация.

1.2. Ответственный за организацию обработки, обеспечение информационной безопасности персональных данных назначается приказом руководителя Организации.

1.3. Ответственный за организацию обработки, обеспечение информационной безопасности персональных данных в своей деятельности руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», нормативными и правовыми актами по вопросам обеспечения безопасности персональных данных, локальными актами Организации по вопросам обработки персональных данных.

2. Обязанности лица, ответственного за организацию обработки персональных данных, обеспечение информационной безопасности в Организации

Лицо, ответственное за организацию обработки, обеспечение информационной безопасности персональных данных в Организации, обязано:

2.1. Определять применимые к деятельности Организации требования законодательства и принятых в его реализацию нормативно-правовых документов, а также внутренние требования по обработке и защите персональных данных.

2.2. Организовывать, планировать и осуществлять внутренний контроль (внутренние аудиты) за соблюдением требований законодательства Российской Федерации при обработке персональных данных, в том числе требований к защите персональных данных, к наличию оснований для обработки персональных данных и установленных сроков обработки персональных данных.

2.3. Обеспечивать контроль за устранением ответственными лицами выявленных несоответствий и нарушений требований обработки персональных данных.

2.4. Доводить до сведения сотрудников положения законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.5. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.6. Осуществлять информационное сопровождение и консультирование по вопросам обработки персональных данных сотрудников, обрабатывающих персональные данные субъектов.

2.7. Принимать решение в конфликтных ситуациях обработки персональных данных и формировать корректирующие действия в отношении политики и правил обработки персональных данных.

2.8. Проводить экспертизу вопросов обработки персональных данных в локальных актах, договорной работе, организации документооборота, информационных системах, при взаимодействии с партнерами и подрядчиками.

2.9. Обеспечивать необходимый уровень компетентности сотрудников в части вопросов персональных данных. Проводить обучение, информирование сотрудников.

2.10. Обеспечивать организацию периодической инвентаризации обрабатываемых персональных данных и проверки соответствия сроков их обработки и хранения срокам, установленным основанием обработки.

2.11. Организовывать процедуры и мероприятия по уничтожению персональных данных как в неавтоматизированной форме, так и с использованием средств автоматизации.

2.12. Обеспечивать взаимодействие с контрольно-надзорным органом по вопросам защиты прав субъектов персональных данных.

2.13. Формировать, согласовывать, готовить на подписание и передавать уведомление об обработке персональных данных в контрольно-надзорный орган по вопросам защиты прав субъектов персональных данных (в случае, если такое уведомление необходимо).

2.14. Обеспечивать организацию работ по выработке и внедрению мероприятий обеспечения информационной безопасности в Организации.

2.15. Вести мониторинг изменений в законодательстве и нормативных документах в области информационной безопасности, а также актуальных угроз и рисков информационной безопасности.

2.16. Обеспечивать актуальность внутренних локальных актов (инструкций, правил и др.) по вопросам информационной безопасности.

2.17. Организация режима конфиденциальности персональных данных и иной информации ограниченного доступа, не составляющей государственную тайну, обрабатываемых в организации.

2.18. Контролировать обеспечение доступности необходимых инструкций, содержащих вопросы информационной безопасности, для сотрудников, имеющих доступ к информационным системам.

2.19. Организовывать обучение, а также вводный, плановый периодический и внеплановый инструктажи сотрудников по вопросам обеспечения информационной безопасности.

2.20. Контролировать результативность выполнения сотрудниками установленных требований по обеспечению безопасности персональных данных в информационных системах.

2.21. Координировать работу администратора ИБ и системного администратора по обеспечению информационной безопасности.

2.22. Организовывать и координировать работу по инцидентам информационной безопасности, принимать решения по инцидентам.

2.23. Формировать отчеты руководству о состоянии защищенности информационных систем персональных данных, информационных ресурсов Организации.

2.24. Контролировать соблюдение правил допуска сотрудников непосредственно к эксплуатации информационных систем, в том числе средств защиты информации.

2.25. Представлять Организацию при проверках надзорных органов, касающихся вопросов информационной безопасности и эксплуатации криптографических средств защиты информации.

3. Права лица, ответственного за организацию обработки, обеспечение информационной безопасности персональных данных в Организации

Лицо, ответственное за организацию обработки, обеспечение информационной безопасности персональных данных в Организации, имеет право:

3.1. Требовать от всех сотрудников выполнения установленной технологии обработки персональных данных, инструкций и локальных актов по вопросам обработки персональных данных и обеспечению их безопасности.

3.2. Участвовать в разработке мероприятий по совершенствованию системы обеспечения безопасности персональных данных.

3.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемых персональных данных и технических средств из состава информационных систем.

3.4. Обращаться к руководителю с предложением о приостановке процесса обработки персональных данных или отстранению от работы сотрудника в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

3.5. Давать свои предложения по совершенствованию организационных, технологических и технических мер защиты персональных данных.

3.6. Привлекать к выполнению аудитов и работ по защите информации внешних подрядчиков.

3.7. Организовывать расследование инцидентов безопасности.

4. Ответственность

4.1. Лицо, ответственное за организацию обработки персональных данных, несет персональную ответственность за соблюдение требований, установленных Федеральным законом от 26.07.2006 №152-ФЗ «О персональных данных», в том числе за обеспечение порядка соблюдения прав субъектов персональных данных и взаимодействия с уполномоченным органом по защите прав субъектов персональных данных.

4.2. Лицо, ответственное за организацию обработки персональных данных, отвечает за качество проводимых им работ по выявлению условий обработки персональных данных, определению применимых требований законодательства и нормативных документов, а также внутренних требований к процессам обработки персональных данных в организации.

4.3. Ответственный несет персональную ответственность в соответствии с действующим законодательством Российской Федерации.

С инструкцией ознакомлен _____