ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 6EF412838E983E1456D185489A3C5439
Владелец: Иконникова Любовь Викторовна
Действителен: с 22.11.2024 до 15.02.2026

УТВЕРЖДАЮ

Директор МАУ ДПО ЦРО

_____ Л.В. Иконникова

«___» _____ 2025 г.

ПОЛОЖЕНИЕ
о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных в муниципальном автономном учреждении дополнительного профессионального образования Петрозаводского городского округа «Центр развития образования»

I. Общие положения

1. Настоящее Положение о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных (далее – Положение) определяет процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок проведения внутреннего контроля (аудита) соответствия обработки персональных данных в функциональных подразделениях муниципального автономного учреждения дополнительного профессионального образования Петрозаводского городского округа «Центр развития образования» (далее — МАУ ДПО ЦРО, Организация) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее — Федеральный закон «О персональных данных»), принятыми в соответствии с ним правовыми актами.

2. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и принятыми в соответствии с ними нормативными правовыми актами.

3. В настоящем Положении используются основные понятия в значениях, определенных статьей 3 Федерального закона «О персональных данных».

II. Общие требования к внутреннему аудиту

2.1. Целями осуществления внутреннего аудита являются:

- оценка общего состояния выполнения в Организации требований по обработке и защите персональных данных, закрепленных законодательно, а также в локальных актах Организации;
- выявление и предотвращение нарушений законодательства в сфере персональных данных.

2.2. Внутренний аудит соответствия обработки персональных данных в Организации требованиям к защите персональных данных (далее – внутренний аудит) осуществляется путем проведения проверок лицом, ответственным за организацию обработки персональных данных в Организации (далее – ответственный за

организацию обработки персональных данных), или комиссией по проведению внутреннего аудита соответствия обработки персональных данных в Организации требованиям к защите персональных данных (далее – комиссия).

2.3. Ответственный за организацию обработки персональных данных назначается приказом руководителя Организации.

2.4. Состав комиссии утверждается приказом руководителя Организации.

2.5. Члены комиссии, получившие допуск к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

III. Порядок осуществления внутреннего аудита

3.1. Проверки соблюдения требований законодательства в сфере персональных данных разделяются на:

- плановые;
- внеплановые.

3.2. Плановые проверки соответствия обработки персональных данных установленным требованиям проводятся согласно Плану внутреннего контроля (аудита) (приложение № 3).

3.3. Внеплановые проверки могут проводится в следующих случаях:

- по результатам расследования выявленных нарушений требований законодательства в сфере персональных данных;
- по результатам внешних контрольных мероприятий, проводимых уполномоченным органом по защите прав субъектов персональных данных.

3.4. Проведение внеплановой проверки организуется ответственным за организацию обработки персональных данных (председателем комиссии), а в его отсутствие - заместителем председателя комиссии в течение трех рабочих дней с даты поступления письменного заявления субъекта персональных данных о нарушении правил обработки персональных данных или с даты выявления нарушений установленных требований.

3.5. Проверка представляет собой комплекс мероприятий, который состоит из следующих этапов:

- подготовка к проведению проверки,
- сбор свидетельств проверки,
- анализ соответствия контрольным параметрам,
- подготовка акта по проверке (приложение №2).

3.6. В ходе подготовки к проведению проверки комиссия или ответственный за организацию обработки персональных данных определяет:

- перечень контрольных параметров,
- объекты контроля (процессы, подразделения, информационные системы персональных данных и т.п.),
- состав участников, привлекаемых для проведения проверки;
- сроки и этапы проведения проверки.

3.7. Типовой перечень контрольных параметров приведен в приложении к настоящему Положению (приложение 1).

3.8. Сбор свидетельств проверки включает:

- анализ организационно-распорядительных и регламентирующих документов по обработке и защите персональных данных.

3.9. Проверки проводятся комиссией непосредственно на месте обработки ПД путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

3.10. Свидетельства проверки сопоставляются с контрольными параметрами для формирования заключения по проверке.

3.11. Общий срок проверки не должен превышать 20 (двадцати) рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более чем на 10 (десять) рабочих дней.

IV. Права комиссии при проведении проверки

4.1. Комиссия (ответственный за организацию обработки персональных данных) для реализации своих полномочий имеет право:

– привлекать к проведению проверок работников Организации;

- запрашивать у руководителей функциональных подразделений Организации и работников Организации информацию и (или) документы, необходимые для осуществления внутреннего аудита;

— требовать от сотрудников, допущенных к работе по обработке персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства РФ в отношении обработки персональных данных;

- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

4.2. Проверки могут проводится с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

V. Порядок фиксирования результатов проверки

5.1. Результаты проведенных проверок оформляются в виде акта внутреннего аудита, составленного по форме согласно Приложению 2 к настоящему Положению, который подписывается ответственным за организацию обработки персональных данных или председателем комиссии, а в его отсутствие — заместителем председателя комиссии, членами комиссии в количестве не менее трех человек и утверждается председателем комиссии.

5.2. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости председатель комиссии докладывает руководителю Организации.

5.3. В целях контроля устранения нарушений может быть проведена повторная проверка.

VI. Заключительные положения.

6.1. Настоящее Положение является нормативным локальным актом и утверждается (либо вводится в действие) приказом руководителя.

6.2. Все изменения и дополнения, вносимые в настоящее Положение, оформляются в письменной форме в соответствии с действующим законодательством РФ.

6.3. Настоящее Положение принимается на неопределенный срок.

6.4. После принятия Положения (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически утрачивает силу.

Приложение 1
к Положению о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных в муниципальном автономном учреждении дополнительного профессионального образования Петрозаводского городского округа «Центр развития образования»

ПЕРЕЧЕНЬ
контрольных параметров проверок соответствия обработки персональных данных установленным требованиям (типовой)

№	Контрольные параметры и объекты проверок
1.	Соответствие установленных в перечне данных категорий персональных данных фактически обрабатываемым в Организации
2.	Соответствие установленных прав доступа к персональным данным полномочиям в рамках трудовых обязанностей работников
3.	Подтверждение факта ознакомления с локальными актами Организации в области обработки и обеспечения безопасности персональных данных
4.	Наличие в договорах с субъектами персональных данных положений, ограничивающих права и свободы субъекта персональных данных, устанавливающих случаи обработки персональных данных несовершеннолетних, если иное не предусмотрено законодательством Российской Федерации, а также положений, допускающих в качестве условия заключения договора бездействие субъекта персональных данных
5.	Наличие в договорах с третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных, выполнения обязанностей, предусмотренных законодательством о персональных данных
6.	Наличие законных целей и оснований обработки всех категорий персональных данных
7.	Выборочные проверки работников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
8.	Соблюдение сроков хранения и порядка уничтожения персональных данных
9.	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных
10.	Необходимость актуализации Уведомления об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, уполномоченного органа по защите прав субъектов персональных данных

Приложение 2
к Положению о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных в муниципальном автономном учреждении дополнительного профессионального образования Петрозаводского городского округа
«Центр развития образования»

АКТ
внутреннего контроля (аудита) соответствия обработки персональных данных требованиям к защите персональных данных в МАУ ДПО «Центр развития образования»

1. Настоящий Акт составлен в том, что «___»_____ 20___ г. ответственным за организацию обработки персональных данных (комиссией в составе: _____) проведена проверка (внутренний аудит) соответствия обработки персональных данных требованиям к защите персональных данных в МАУ ДПО ЦРО.

2. Проверка осуществлялась в соответствии с требованиями:
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных);
- постановления Правительства РФ от 01.11.20212 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Политики защиты и обработки персональных данных МАУ ДПО ЦРО;
- Положения об обработке и защите персональных данных работников МАУ ДПО ЦРО.

3. Результаты рассмотрения вопросов по предметам аудита:

Предмет аудита	Результат рассмотрения	Примечание

Выявленные нарушения:
_____
_____
_____
_____
_____
_____

Меры по устранению нарушений:
_____
_____
_____
_____
_____

Срок устранения нарушений: _____ .

Ответственный за организацию обработки персональных данных _____
/ Комиссия в составе:
Председатель: _____
Члены комиссии: _____
_____
_____

Приложение 3
к Положению о внутреннем контроле (аудите) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных в муниципальном автономном учреждении дополнительного профессионального образования Петрозаводского городского округа
«Центр развития образования»

ПЛАН
внутреннего контроля (аудита) соответствия обработки персональных данных установленным требованиям законодательства в сфере обработки персональных данных в МАУ ДПО «Центр развития образования»

№	Мероприятие	периодичность	исполнитель
1	Контроль компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов)	постоянно	Заместитель директора Системный администратор, техник-программист
2	Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных	раз в 3 года	Системный администратор, техник-программист
3.	Организация анализа и пересмотра имеющихся угроз безопасности ЗИ, а также предсказание появления новых угроз	ежегодно	Системный администратор, техник-программист
4.	Проведение внутренних проверок на предмет соответствия обработки персональных данных требованиям к защите персональных данных	ежегодно	Ответственный за организацию обработки персональных данных, либо комиссия
5.	Поддержание в актуальном состоянии документа «Список лиц, доступ которых к защищаемой информации необходим для выполнения служебных (трудовых) обязанностей»	ежемесячно	Ответственный за организацию обработки персональных данных
6.	Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на элементах ИС	ежемесячно	Системный администратор, техник-программист
7.	Проведение мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИС и по реагированию на компьютерные инциденты в них	постоянно	Системный администратор, техник-программист
8.	Контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения	ежемесячно	Заместитель директора Системный администратор, техник-программист
9.	Контроль наличия и местонахождения машинных носителей информации	ежемесячно	Заместитель директора Начальники отделов
10.	Контроль выполнения условий и сроков	ежемесячно	Заместитель директора

	действия сертификатов соответствия на средства защиты информации		Системный администратор, техник-программист
11.	Контроль за соблюдением режима безопасности помещений, в которых осуществляется обработка персональных данных	ежеквартально	Заместитель руководителя
12.	Контроль за соблюдением режима безопасности помещений, в которых размещена информационная система	ежеквартально	Ответственный за организацию обработки персональных данных
13.	Контроль сохранности носителей защищаемой информации	ежеквартально	Заместитель руководителя Начальники отделов/функциональных подразделений
14.	Поддержание в актуальном состоянии организационно-распорядительных документов	ежеквартально	Ответственный за организацию обработки персональных данных