УТВЕРЖДЕНО:
Директор ООО «ЛРЦ «Клиника Инсайт»

_____ Р.Д. Миназов

12.09.2022 г.

Положение
об осуществлении внутреннего контроля и (или) аудита соответствия обработки персональных данных законодательству Российской Федерации о персональных данных, требованиям к защите персональных данных

1. Общие положения

1.1. Настоящие Положение разработано в соответствии с пунктом 4 части 1 статьи 18.1 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон о персональных данных), а также иными правовыми актами, принимаемыми в соответствии с законодательством в сфере персональных данных, и определяет основания, порядок и формы проведения внутреннего контроля и (или) аудита соответствия обработки персональных данных в ООО «ЛРЦ «Клиника Инсайт» (Озарение) (далее - организация) законодательству Российской Федерации о персональных данных, требованиям к защите персональных данных (далее - установленные требования).

1.2. Основными целями внутреннего контроля и аудита соответствия обработки персональных данных установленным требованиям являются оценка соблюдения требований законодательства (в частности, Закона о персональных данных), минимизация правовых и репутационных рисков, выявление уязвимостей в процессах, а также обеспечение безопасности данных для защиты прав субъектов персональных данных и подготовки к проверкам.

1.3. Под внутренним контролем понимается регулярный мониторинг соответствия обработки персональных данных установленным требованиям, направленный на выявление текущих нарушений и дальнейшее их устранение.

1.4. Под внутренним аудитом понимается комплексная оценка эффективности системы обработки персональных данных, поиск рисков, улучшение процессов обработки и предотвращения рисков.

2. Порядок осуществления внутреннего контроля

2.1. Внутренний контроль соответствия обработки персональных данных установленным требованиям (далее - внутренний контроль) осуществляется комиссией, создаваемой на основании приказа руководителя организации.

2.2. Внутренний контроль подразделяется на плановые и внеплановые проверки.

2.3. Плановые проверки проводятся согласно ежегодно утверждаемому плану мероприятий внутреннего контроля.

2.4. Непосредственно перед началом проведения плановой проверки, за 10 рабочих дней, секретарем комиссии направляются уведомления руководителям структурных подразделений, в которых планируется проведение внутреннего контроля.

2.5. Внеплановые внутренние проверки могут проводиться 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.

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

- подготовка к проведению проверки;
- сбор свидетельств проверки;
- анализ соответствия контрольным параметрам;
- подготовка заключения по проверке.

2.7. В ходе подготовки к проведению проверки комиссия определяет:

- границы и описание области, подвергающейся проверке;
- 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.

2.8. Типовой перечень контрольных параметров приведен в приложении к настоящему Положению.

2.9. Сбор свидетельств проверки включает:

- анализ организационно-распорядительных и регламентирующих документов по обработке и защите персональных данных;
- опрос персонала, участвующего в процессах обработки персональных данных, обслуживании и эксплуатации информационных систем персональных данных.

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

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

2.12. Общий срок проверки не должен превышать 30 рабочих дней. При необходимости срок проведения проверки может быть продлен, но не более чем на 10 рабочих дней.

2.13. По результатам внутреннего контроля комиссией при необходимости проводится заседание. Решения, принятые на заседаниях комиссии, оформляются протоколом.

2.14. В целях контроля устранения выявленных нарушений комиссия проводит повторную проверку.

3. Права комиссии при осуществлении внутреннего контроля

3.1. Комиссия для реализации своих полномочий имеет право:

- привлекать к проведению проверок работников организации и работников подведомственных организаций;
- запрашивать у работников организации и подведомственных организаций необходимую информацию;
- принимать меры по устранению выявленных нарушений выполнения требований к защите персональных данных в организации;
- 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 отношении обработки персональных данных.

4. Порядок проведения внутреннего аудита

4.1. Внутренний аудит соответствия обработки персональных данных установленным требованиям (далее - внутренний аудит) осуществляется ответственным за организацию обработки персональных данных, назначаемым приказом руководителя организации (далее - ответственное должностное лицо).

4.2. Внутренний аудит проводится не реже одного раза в год на основании распорядительного акта руководителя организации.

4.3. Внутренний аудит представляет собой комплекс мероприятий, который состоит из следующих этапов:

- подготовка и планирование проверки;
- проведение проверки (инвентаризация);
- оформление результатов проверки;
- устранение нарушений, выявленных в ходе проверки.

4.4. В ходе подготовки и планирования проверки:

- руководителем организации издается приказ о проведении аудита, в котором определяются сроки проверки;
- ответственным должностным лицом определяются цели проверки, составляется план проверки и определяется перечень структурных подразделений, подлежащих проверке.

4.5. В ходе проведения проверки (инвентаризации) ответственным должностным лицом осуществляется:

- проверка наличия и актуальности локальных актов организации (Политика обработки персональных данных, приказы, журналы и т. п.);
- анализ согласий на обработку персональных данных и законности оснований обработки персональных данных;
- проверка информационных систем, контроль доступа, защита от утечек;
- оценка информированности сотрудников (инструктажи).

4.6. Оформление результатов проверки производится путем:

- составления акта проверки, в котором фиксируются все выявленные нарушения и замечания;
- подготовки отчета с выводами и рекомендациями по улучшению.

4.7. В ходе устранения нарушений, выявленных в ходе проверки:

- руководителем организации издается приказ о мерах по устранению выявленных нарушений;
- руководителями структурных подразделений и ответственными должностными лицами реализуются корректирующие действия в установленные сроки.

5. Права ответственного должностного лица при осуществлении внутреннего аудита

5.1. Ответственное должностное лицо для реализации своих полномочий имеет право:

- запрашивать и получать от работников информацию, локальные акты, договоры и иные документы, связанные с обработкой персональных данных;
- осуществлять беспрепятственный доступ в помещения, используемые для обработки персональных данных, включая места хранения материальных носителей (архивы, кабинеты);
- проверять рабочие места, компьютерную технику и информационные системы на предмет соблюдения мер защиты персональных данных;
- проводить опросы работников по вопросам соблюдения требований безопасности.

6. Порядок фиксирования результатов внутреннего контроля и (или) аудита

6.1. Факт проведения проверок и результаты проверки фиксируются в журнале проведения внутреннего контроля и (или) аудита соответствия обработки персональных данных

установленным требованиям.

6.2. Протоколы внутреннего контроля, акты внутреннего аудита, докладные записки по итогам контрольных мероприятий и отчеты хранятся в кабинет руководителя организации.

7. Заключительные положения

7.1. Внутренний контроль и аудит могут проводиться с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

7.2. Настоящее Положение вступает в силу с даты его утверждения.

7.3. Настоящее Положение может быть изменено и (или) дополнено, в том числе в случае изменения законодательства Российской Федерации.

7.4. Изменения и дополнения к настоящему Положению вступают в силу с даты их утверждения в установленном порядке.

7.5. Настоящее Положение доводится до сведения всех работников, осуществляющих обработку персональных данных, персонально под подпись.

Приложение № 1

УТВЕРЖДЕНО:
Директор ООО «ЛРЦ «Клиника Инсайт»

_____ Р.Д. Миназов

01.03.2026 г.

План-график
осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям

ООО «ЛРЦ «Клиника Инсайт»

Период проверки	Структурное подразделение	Наименование контрольного мероприятия
1	2	3
01.03.27 г. – 30.03.27 г.	Институт	Согласно перечня контрольных параметров (Приложение №2)
01.03.28 г. – 30.03.28 г.	Институт	Согласно перечня контрольных параметров (Приложение №2)
01.03.29 г. – 30.03.29 г.	Институт	Согласно перечня контрольных параметров (Приложение №2)
01.03.30 г. – 30.03.30 г.	Институт	Согласно перечня контрольных параметров (Приложение №2)
01.03.31 г. – 30.03.31 г.	Институт	Согласно перечня контрольных параметров (Приложение №2)

Секретарь комиссии _____/_____/

Приложение №2

Перечень контрольных параметров проверок в области обработки и обеспечения безопасности персональных данных

в ООО «ЛРЦ «Клиника Инсайт»

N п/п	Контрольные параметры и объекты проверок
1	Соответствие установленных в перечне персональных 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 третьими лицами положений, касающихся обеспечения конфиденциальности и безопасности персональных данных
5	Наличие законных целей и оснований обработки всех категорий персональных данных
6	Выборочные проверки сотрудников на предмет знания организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных
7	Соблюдение сроков хранения и порядка уничтожения персональных данных
8	Соблюдение процедур и сроков подготовки ответов на обращения субъектов персональных данных
9	Необходимость актуализации Уведомления уполномоченного органа по защите прав субъектов персональных данных

Приложение № 3

Журнал(форма)
проведения внутреннего контроля и (или) аудита соответствия обработки персональных данных установленным требованиям

ООО «ЛРЦ «Клиника Инсайт»

№ п/п	Вид проверки (плановая или внеплановая)	Дата проведения проверки	Основание проверки	Заключение по факту проверки (кратко)	Подпись председателя комиссии/ответственного должностного лица
1	2	3	4	5	6

Приложение № 3

УТВЕРЖДЕНО:
Директор ООО «ЛРЦ «Клиника Инсайт»

_____ Р.Д. Миназов

«__»_____20____ г.

Акт
внутреннего аудита соответствия обработки персональных данных установленным требованиям

№ _____ «___»_____20____г.

1. Период проведения внутреннего аудита соответствия обработки персональных данных установленным требованиям: с «____»_____20___г. по «___»_____20___г.

2. Внутренний аудит проведен:_____.
(должность, Ф. И. О.)

3. Проверены локальные нормативные акты:
_____
_____
_____.
(указать перечень локальных нормативных актов)

4. Проведены контрольные мероприятия:

№ п/п	Наименование проверяемого структурного подразделения	Наименование контрольного мероприятия	Результат контрольного мероприятия
1	2	3	4

5. Заключение по результатам внутреннего аудита: _____.
(вписать нужное)

6. Рекомендовано: _____.
(вписать нужное)

Ответственный за
организацию обработки
персональных данных _____ /_____/

Приложение №5

Лист
ознакомления с положением

С положением ознакомлены:

№ п/п	Ф. И. О. работника	Дата	Подпись
1	2	3	4