Приложение № 1 к приказу № 1015 от 15.10.2024 года «Об утверждении Положения о внутреннем контроле и (или) аудите соответствия обработки персональных данных в ООО «Центр ДНК исследований» требованиям законодательства в сфере обработки персональных данных.

УТВЕРЖДЕНО Приказом по ООО «Центр ДНК исследований» № 1015 от 15.10.2024

**Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в ООО «Центр ДНК исследований» требованиям законодательства в сфере обработки персональных данных**

**1. Общие положения**

1.1. Настоящее Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в ООО «Центр ДНК исследований» требованиям законодательства в сфере обработки персональных данных (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Положение определяет порядок осуществления внутреннего контроля соответствия обработки персональных данных в ООО «Центр ДНК исследований» (далее – медицинская организация) требованиям к защите персональных данных, установленным законодательством Российской Федерации.

1.3. Исполнение Положения обязательно для всех работников медицинской организации, осуществляющих обработку персональных данных, как без использования средств автоматизации, так и в информационных системах обработки персональных данных.

1.4. В Положении используются основные понятия в значениях, определенных статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

**Внутренний контроль соответствия обработки персональных данных** – контроль соответствия обработки персональных данных в медицинской организации требованиям законодательства в сфере обработки персональных данных, проводимый силами медицинской организации в соответствии с Положением и другими локальными нормативными актами организации.

**Внутренний аудит соответствия обработки персональных данных** – контроль соответствия обработки персональных данных в медицинской организации требованиям законодательства в сфере обработки персональных данных.

**2. Порядок проведения внутреннего контроля**

2.1. Внутренний контроль соответствия обработки персональных данных осуществляется комиссией по плану мероприятий внутреннего контроля, утверждаемому ежегодно руководителем медицинской организации.

2.2. Мероприятия внутреннего контроля могут быть внеплановыми по решению комиссии, если есть фактические основания полагать, что процедура обработки персональных данных в медицинской организации не соответствует требованиям законодательства Российской Федерации.

2.3. Состав комиссии утверждается руководителем медицинской организации.

2.4. Мероприятия внутреннего контроля могут осуществляться как непосредственно на рабочих местах исполнителей, участвующих в обработке персональных данных, так и путем направления запросов и рассмотрения документов, необходимых для осуществления внутреннего контроля.

2.5. При проведении мероприятия внутреннего контроля должны быть полностью, объективно и всесторонне установлены:

• порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

• порядок и условия применения средств защиты информации;

• эффективность принимаемых мер по обеспечению безопасности персональных данных;

• состояние учета машинных носителей персональных данных;

• соблюдение правил доступа к персональным данным;

• наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

• мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

• осуществление мероприятий по обеспечению целостности персональных данных.

2.6. Комиссия при проведении внутреннего контроля имеет право:

• запрашивать у работников, осуществляющих обработку персональных данных, информацию и (или) документы, необходимые для осуществления внутреннего контроля;

• требовать у ответственных за обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных

• принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

• вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке в образовательной организации;

• вносить предложения о привлечении к дисциплинарной ответственности работников, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.7. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность.

2.8. Мероприятие внутреннего контроля не может длиться больше 10 рабочих дней. Срок мероприятия может быть продлен распорядительным актом руководителя медицинской организации при наличии оснований, не позволяющих закончить контрольное мероприятие за 10 рабочих дней.

**3. Оформление итогов внутреннего контроля**

3.1. Результаты внутреннего контроля соответствия обработки персональных данных оформляются комиссий в виде акта внутреннего контроля, составленного по форме согласно Приложению к Положению. Члены комиссии обязаны составлять докладные записки по итогам контрольных мероприятий, если это предусматривает план мероприятий внутреннего контроля или распорядительный акт директора медицинской организации.

3.2. Акт внутреннего контроля подписывается всеми членами комиссии.

3.3. Выявленные в ходе внутреннего контроля нарушения фиксируются в акте внутреннего контроля с предложениями мероприятий по устранению нарушений и сроков их выполнения.

3.4. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости комиссия докладывает на очередном совещании при руководителе медицинской организации, если иное не установлено распорядительным актом руководителя медицинской организации.

3.5. Акты внутреннего контроля, докладные записки по итогам контрольных мероприятий хранятся в запирающемся шкафу в кабинете заместителя руководителя медицинской организации.

**4. Порядок проведения внутреннего аудита**

4.1. Внутренний аудит соответствия обработки персональных данных проводится в случаях, когда медицинская организация не может объективно оценить соответствие обработки персональных данных в медицинской организации требованиям законодательства в сфере обработки персональных данных.

4.2. Внутренний аудит организуется на основании распорядительного акта руководителя медицинской организации

4.3 Внутренний аудит проводит организация, которая в соответствии со своими учредительными документами занимается оценкой рисков в обработке персональных данных и возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

4.4. На время проведения внутреннего аудита руководитель медицинской организации назначает ответственного, который должен взаимодействовать с организацией, проводящей аудит (далее – аудитор).

4.5. Ответственный обязан:

• обеспечить аудитора всей необходимой информацией;

• организовать условия для работы;

• оказывать помощь при возникновении трудностей;

• контролировать работу аудитора;

• принимать все отчеты аудитора и доводить их до сведения руководителя медицинской организации.

4.6. Действия и обязанности аудитора определяются заключенным договором оказания услуг по проведению внутреннего аудита.

4.7. Документы внутреннего аудита, в том числе итоговые отчеты, хранятся в запирающемся шкафу в кабинете руководителя медицинской организации.

Приложение к положения о внутреннем контроле и (или) аудите соответствия обработки персональных данных в ООО «Центр ДНК исследований» требованиям законодательства в сфере обработки персональных данных

**Акт №\_\_\_\_ от \_\_\_\_\_\_\_\_**

**внутреннего контроля соответствия обработки персональных данных**

**в ООО «Центр ДНК исследований» требованиям законодательства**

**в сфере обработки персональных данных**

Комиссия ООО «Центр ДНК исследований» в составе:

Директор

Члены комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

провела внутренний контроль соответствия обработки персональных данных в ООО «Центр ДНК исследований» требованиям законодательства в сфере обработки персональных данных в соответствии с планом внутреннего контроля на год, утвержденным приказом директором ООО «Центр ДНК исследований»

В ходе контрольных мероприятий проверены:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ответственный за исполнение:

Подписи членов комиссии

Приложение № 2 к приказу № 1015 от 15.10.2024 года «Об утверждении Положения о внутреннем контроле и (или) аудите соответствия обработки персональных данных в ООО «Центр ДНК исследований» требованиям законодательства в сфере обработки персональных данных

УТВЕРЖДЕНО Приказом по ООО «Центр ДНК исследований» № 1015 от 15.10.2024

**План-график мероприятий внутреннего контроля соответствия обработки персональных данных на 2024 год**

|  |  |  |
| --- | --- | --- |
| Мероприятие | Ответственный | Срок исполнения |
| Проверка соблюдения правил доступа к персональным данным  Проверка соблюдения режима защиты | Ответственный за обработку персональных данных;  системный администратор | 01.06.2024,01.07.2024,01.08.2024, 01.09.2024, 01.10.2024, 01.11.2024, 22.12.2024 |
| Проверка выполнения антивирусной политики  Проверка обновления ПО и единообразия применяемого ПО на всех устройствах, используемых при обработке персональных данных | Ответственный за обработку персональных данных;  системный администратор | 20.06.2024, 20.09.2024, 20.12.2024 |
| Проверка актуальности локальных нормативных актов в сфере обработки персональных данных | Ответственный за обработку персональных данных;  системный администратор | 15.05.2024, 30.09.2024 |
| Рассмотрение итогов мероприятий внутреннего контроля | Ответственный за обработку персональных данных | 20.12.2024г |

Приложение № 3 к приказу № 1015 от 15.10.2024 года «Об утверждении Положения о внутреннем контроле и (или) аудите соответствия обработки персональных данных в ООО «Центр ДНК исследований» требованиям законодательства в сфере обработки персональных данных

УТВЕРЖДЕНО Приказом по ООО «Центр ДНК исследований» № 1510 от 15.10.2024

**План-график мероприятий внутреннего контроля соответствия обработки персональных данных на 2025 год**

|  |  |  |
| --- | --- | --- |
| Мероприятие | Ответственный | Срок исполнения |
| Проверка соблюдения правил доступа к персональным данным  Проверка соблюдения режима защиты | Ответственный за обработку персональных данных;  системный администратор | 01.02.2025, 01.03.2025, 01.04.2025, 04.05.2025, 01.06.2025,01.07.2025,01.08.2025, 01.09.2025, 01.10.2025, 01.11.2025, 22.12.2025 |
| Проверка выполнения антивирусной политики  Проверка обновления ПО и единообразия применяемого ПО на всех устройствах, используемых при обработке персональных данных | Ответственный за обработку персональных данных;  системный администратор | 20.03.2025, 20.06.2025, 20.09.2025, 20.12.2025 |
| Проверка актуальности локальных нормативных актов в сфере обработки персональных данных | Ответственный за обработку персональных данных;  системный администратор | 10.01.2025, 15.05.2025, 30.09.2025 |
| Рассмотрение итогов мероприятий внутреннего контроля | Ответственный за обработку персональных данных | 20.12.2025г |