

**Положение
о внутреннем контроле и (или) аудите соответствия обработки
персональных данных в государственном казенном учреждении
социального обслуживания населения Астраханской области
«Комплексный центр социального обслуживания населения,
Наримановский район, Астраханская область»**

1. Общие положения

1.1. Настоящее Положение о внутреннем контроле и (или) аудите соответствия обработки персональных данных в ГКУСОН АО «КЦСОН, Наримановский район» 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 ГКУСОН АО «КЦСОН, Наримановский район» (далее – центр) требованиям к защите персональных данных, установленным законодательством Российской Федерации.

1.3. Исполнение Положения обязательно для всех работников центра, 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 центре требованиям законодательства в сфере обработки персональных данных, проводимый силами центра в соответствии с Положением и другими локальными нормативными актами организации.

2. Порядок проведения внутреннего контроля

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

2.2. Мероприятия внутреннего контроля могут быть внеплановыми по решению комиссии, если есть фактические основания полагать, что

процедура обработки персональных данных в центре не соответствует требованиям законодательства Российской Федерации.

2.3. Состав комиссии утверждается руководителем центра.

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 центре;
- 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 центра 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 комиссией 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 центра.

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 выявленных нарушениях, по мере необходимости комиссия докладывает на очередном совещании при руководителе центра, если иное не установлено распорядительным актом руководителя центра.

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

4. Порядок проведения внутреннего аудита

4.1. Внутренний аудит соответствия обработки персональных данных проводится в случаях, когда центр не может объективно оценить соответствие обработки персональных данных в центре требованиям законодательства в сфере обработки персональных данных.

4.2. Внутренний аудит организуется на основании распорядительного акта руководителя центра.

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 центра 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 центра.

4.6. Действия и обязанности аудитора определяются заключенным договором - принимать все отчеты аудитора и доводить их до сведения руководителя центра.

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

4.8. Документы внутреннего аудита, в том числе итоговые отчеты, хранятся в запирающемся шкафу в кабинете заместителя руководителя центра.

Приложение к приказу № 37-П от 19.09.2025 г.
Положению о внутреннем контроле и (или) аудите соответствия обработки
персональных данных в ГКУСОН АО «КЦСОН, Наримановский район» требованиям
законодательства в сфере обработки персональных данных (как образец)

Акт № ____ от _____

внутреннего контроля соответствия обработки персональных данных в
ГКУСОН АО «КЦСОН, Наримановский район» требованиям
законодательства в сфере обработки персональных данных

Комиссия ГКУСОН АО «КЦСОН, Наримановский район» в составе:

Заместителя директора - Глаголевой И.Г.
Специалиста по кадрам - Тимофеевой Т.В.
Делопроизводителя - Ревиной Т.В.

провела внутренний контроль соответствия обработки персональных
данных в ГКУСОН АО «КЦСОН, Наримановский район» требованиям
законодательства в сфере обработки персональных данных в соответствии
с планом внутреннего контроля на ____ год, утвержденным приказом
директора ГКУСОН АО «КЦСОН, Наримановский район» от
_____. № _____. (как образец)

В ходе контрольных мероприятий проверены:

- документы, определяющие основания обработки персональных данных; -
утвержденный перечень работников ГКУСОН АО «КЦСОН,
Наримановский район», имеющих доступ к персональным данным в силу
своих служебных обязанностей;
- своевременность мероприятий по уничтожению персональных данных,
обрабатываемых в ГКУСОН АО «КЦСОН, Наримановский район», в связи
с достижением целей обработки или утраты необходимости в достижении
этих целей;
- отсутствие неправомерно размещенных персональных данных граждан
на сайте ГКУСОН АО «КЦСОН, Наримановский район» и иных
общедоступных местах.

Выявленные нарушения: (как образец)

1. Политика обработки персональных данных ГКУСОН АО «КЦСОН,
Наримановский район» не соответствует требованиям законодательства –

нет положений о согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2. Меры по устранению нарушений: (как пример)

1. Необходимо внести изменения в Политику обработки персональных данных ГКУСОН АО «КЦСОН, Наримановский район» и привести нормы о согласии на обработку персональных данных в соответствие с действующим законодательством.

2. Срок устранения нарушений: _____.

Ответственный за исполнение: Ревина Т.В.

Подписи членов комиссии:

Заместитель директора _____ (ФИО)