

**Муниципальное бюджетное учреждение культуры
«Районный дом культуры и спорта»
муниципального образования
Староминский район**

ПРИКАЗ

26.05.2023 года

№197

ст-ца Староминская

**О внутреннем контроле соответствия обработки персональных данных
в муниципальном бюджетном учреждении культуры «Районный дом
культуры и спорта муниципального образования Староминский район**

В целях исполнения требований Федерального закона от 27 июня 2006 года № 152-ФЗ «О персональных данных» приказываю:

1. Утвердить Положение о внутреннем контроле соответствия обработки персональных данных в муниципальном бюджетном учреждении культуры «Районный дом культуры и спорта» муниципального образования Староминский район (прилагается).

2. Создать комиссию по проведению внутреннего контроля соответствия обработки персональных данных в составе:

Председатель:

Кулишова

Ольга Николаевна

- директор муниципального бюджетного учреждения культуры «Районный дом культуры и спорта» образования Староминский район, председатель;

Лушкова

Ольга Николаевна

Члены комиссии:

Лукавченко

Анастасия Вадимовна

Бирюк

Наталья Ивановна

- специалист по кадрам, секретарь;

- методист МБУК «РДКС» МО Староминский район;

- художественный руководитель МБУК «РДКС» МО Староминский район;

Латушко

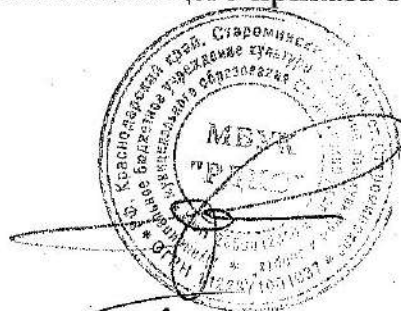
Марина Сергеевна

- заместитель директора МБУК «РДКС» МО Староминский район;

3. Настоящий приказ подлежит размещению в информационно-телекоммуникационной сети «Интернет».

4. Контроль за выполнением настоящего приказа оставляю за собой.

Директор «МБУК «РДКС»



О.Н. Кулишова

И. Бирюков А.И.
В. Лукавиченко А.В.
Е. Катученко М.С.

Приложение 1

УТВЕРЖДЕНО:

приказом муниципального бюджетного учреждения культуры «Районный дом культуры и спорта» муниципального образования Староминский район
от 26 мая 2023 года №197

Положение
о внутреннем контроле соответствия обработки персональных данных в
муниципальном бюджетном учреждении культуры «Районный дом
культуры и спорта» муниципального образования Староминский район

1. Общие положения

1.1. Настоящее Положение о внутреннем контроле соответствия обработки персональных данных в муниципальном бюджетном учреждении культуры «Районный дом культуры и спорта» муниципального образования Староминский район (далее- МБУК «РДКС») 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 муниципальном бюджетном учреждении культуры «Районный дом культуры и спорта» муниципального образования Староминский район(далее – МБУК «РДКС») требованиям к защите персональных данных, установленным законодательством Российской Федерации.

1.3. Исполнение Положения обязательно для всех работников учреждения, 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».

1.5. Внутренний контроль соответствия обработки персональных данных – контроль соответствия обработки персональных данных в МБУК «РДКС» требованиям законодательства в сфере обработки персональных данных, проводимый силами отдела культуры в соответствии с Положением и другими локальными нормативными актами учреждения.

1.6. Для обработки ПДн, связанных с приемом граждан по личным вопросам, а также для работы с корреспонденцией заявителей, используется информационная система персональных данных без использования средств автоматизации (далее – ИСПДн) «Регистрация обращений граждан», «Журнал личного приема граждан».

1.7. Пользователями ИСПДн (далее – Пользователь) являются сотрудники отдела культуры, участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

1.8. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдения условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн проводятся в следующих целях:

1.8.1 проверка выполнения требований организационно-распорядительной документации по защите информации в министерстве и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.8.2 оценка уровня осведомленности и знаний работников отдела культуры в области обработки и защиты персональных данных;

1.8.3 оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

2.1. Проверки соответствия обработки ПДн установленным требованиям в отделе культуры разделяются на следующие виды:

- плановые;
- внеплановые.

2.2. Плановые контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн отдела культуры.

2.3. Внеплановые контрольные мероприятия проводятся на основании решения комиссии (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и создании комиссии по информационной безопасности может быть принято в следующих случаях:

2.3.1. по результатам расследования инцидента информационной безопасности;

2.3.2. по результатам внешних контрольных мероприятий, проводимых регулирующими органами.

3. Порядок проведения внутреннего контроля

3.1. Внутренний контроль соответствия обработки персональных данных осуществляется комиссией по плану мероприятий внутреннего контроля, утверждаемому ежегодно директором МБУК «РДКС», форма которого установлена в Приложении 1 к настоящему.

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

3.3. Состав комиссии утверждается директором учреждения.

3.4. 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.

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

- Контроль соблюдения правил доступа к ПДн
- Контроль соблюдения режима защиты
- Контроль выполнения антивирусной политики
- Контроль выполнения парольной политики
- Контроль соблюдения режима защиты при подключении к сетям общего пользования
- Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн
- Поддержание в актуальном состоянии нормативно-организационных документов
- Хранение бумажных носителей с персональными данными
- Контроль запрета на использование беспроводных соединений
- Проверка актуальности информации, содержащейся в Уведомлении об обработке персональных данных, предоставленной в Роскомнадзор.

3.6. 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 учреждении;

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

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

3.8. Общий срок проведения внутреннего контроля не должен превышать пяти рабочих дней. При необходимости срок проведения может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Акте, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление итогов внутреннего контроля

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

4.2. Результаты внутреннего контроля соответствия обработки персональных данных оформляются комиссией в виде акта внутреннего контроля, составленного по форме согласно Приложению к Положению.

4.3. Акт внутреннего контроля подписывается всеми членами комиссии.

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

4.5. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости комиссия докладывает начальнику отдела культуры.

4.6. Акты внутреннего контроля по итогам контрольных мероприятий хранятся в запирающемся шкафу в кабинете №39 по адресу 353600 Краснодарский край станица Староминская ул.Калинина,2.

Директор «МБУК «РДКС»



О.Н. Кулишова

Приложение 1

к Положению о внутреннем контроле соответствия обработки персональных данных в муниципальном бюджетном учреждении культуры «Районный дом культуры и спорта» муниципального образования Староминский район

Форма

План проведения внутреннего контроля соответствия обработки персональных данных в муниципальном бюджетном учреждении культуры «Районный дом культуры и спорта» муниципального образования Староминский район

№	Мероприятие	Регулярность проведения
1.	Контроль соблюдения правил доступа к ПДн	Ежегодно
2.	Контроль соблюдения режима защиты	Ежегодно
3.	Контроль выполнения антивирусной политики	Ежегодно
4.	Контроль выполнения парольной политики	Ежегодно
5.	Контроль соблюдения режима защиты при подключении к сетям общего пользования	Ежегодно
6.	Хранение бумажных носителей с персональными данными	Ежегодно
7.	Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно
8.	Поддержание в актуальном состоянии нормативно-организационных документов	1 раз в три года или по мере обновления законодательства РФ
9.	Контроль запрета на использование беспроводных соединений	Ежегодно
10.	Проверка актуальности информации, содержащейся в Уведомлении об обработке персональных данных, предоставленной в Роскомнадзор.	Ежегодно

Приложение 2

к Положению о внутреннем контроле соответствия обработки персональных данных в муниципальном бюджетном учреждении культуры «Районный дом культуры и спорта» муниципального образования Староминский район

Акт № _____

проведения внутренней проверки соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном бюджетном учреждении культуры «Районный дом культуры и спорта» муниципального образования Староминский район

Дата составления: « ____ » _____ 20 ____ г.

Место проведение проверки: _____

Комиссия, назначенная приказом отдела культуры и искусства администрации муниципального образования Староминский район от « ____ » _____ 20 ____ № _____ в составе:

председателя комиссии: _____

членов комиссии: _____

руководствуясь «Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, положением о порядке обработки персональных данных субъектов» провела проверку условий обработки персональных данных в муниципальном бюджетном учреждении культуры «Районный дом культуры и спорта» муниципального образования Староминский район (далее – оператор). В ходе проверки:

– проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (статья 18.1, статья 19) и принятыми в соответствии с ним локальными актами оператора, определяющих его политику в отношении обработки персональных данных;

– проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных, утвержденных постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– проведен анализ реализации оператором организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; – проведен анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных на соответствие Техническому паспорту информационной системы.

Выявленные нарушения

ЗАКЛЮЧЕНИЕ комиссии:

Обработка персональных данных соответствует (не соответствует) требованиям к защите персональных данных и политике оператора в отношении обработки персональных данных, установленным в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, а также локальными актами оператора.

Председатель комиссии:

Члены комиссии: