МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ «СТАРОМИНСКИЙ ИСТОРИКО-КРАЕВЕДЧЕСКИЙ МУЗЕЙ» МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ СТАРОМИНСКИЙ РАЙОН

ПРИКАЗ

27.03.2023 года № 78

ст-ца Староминская

Об утверждении инструкций

В соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и подпунктом "б" пункта 1 перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211, п р и к а з ы в а ю:

1. Утвердить:

1.1. Инструкцию по антивирусной защите в информационных системах персональных данных муниципального бюджетного учреждения культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение 1);

1.2. Инструкцию пользователя информационной системы персональных данных при возникновении нештатных ситуаций муниципального бюджетного учреждения культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение **2**).

1.3. Инструкция Пользователя информационной системы персональных данных в муниципальном бюджетном учреждении культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение 3).

1.4. Инструкция по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных в муниципальном бюджетном учреждении культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение 4).

1.5. Инструкция по учёту и хранению съёмных носителей персональных данных в муниципальном бюджетном учреждении культуры

«Староминский историко-краеведческий музей» МО Староминский район (приложение 5).

1.6. Инструкция по порядку уничтожения и обезличивания персональных данных в ИСПДн муниципального бюджетного учреждения культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение 6).

1.7. Инструкция по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных муниципального бюджетного учреждения культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение 7).

1.8. Иструкция по проведению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в муниципальном бюджетном учреждении культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение 8).

1.9. Инструкция по организации резервирования и восстановления программного обеспечения, баз персональных данных информационной системы персональных данных в муниципальном бюджетном учреждении культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение 9).

1.10. Инструкцию ответственного за организацию обработки персональных данных в муниципальном бюджетном учреждении культуры «Староминский историко-краеведческий музей» МО Староминский район (приложение 10).

1.11. Инструкция пользователя информационной системы персональных данных (приложение 11).

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

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор
муниципального бюджетного учреждения культуры
«Староминский историко-краеведческий музей»
муниципального образования Староминский район А.Н.Жаловага

Приложение 1

УТВЕРЖДЕНО:
[2]приказом отдела культуры и искусства
администрации муниципального
образованияСтароминский район
от 27 марта 2023 года №79

Инструкция
по антивирусной защите в информационных системах персональных данных отдела культуры и искусстваадминистрации МО Староминский район

1. Настоящая инструкция разработана с целью защиты персональных данных от несанкционированного, в том числе случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

2. Пользователи ИСПДн при работе со съемными носителями обязаны перед началом работы осуществить их проверку на предмет наличия компьютерных вирусов.

3. Ответственный за обеспечение безопасности персональных данных настраивает антивирусное средство на автоматическое обновление и ведет за ним контроль.

4. Ответственный за обеспечение безопасности персональных данных проводит периодическое тестирование всех элементов ИСПДн и установленного программного обеспечения на предмет наличия компьютерных вирусов.

5. Использование для обработки и хранения персональных данных неучтенных носителей запрещается.

6. При обнаружении компьютерного вируса пользователи ИСПДн обязаны немедленно поставить в известность ответственного за обеспечение безопасности персональных данных и прекратить какие-либо действия в соответствующей ИСПДн.

7. Ответственный за обеспечение безопасности персональных данных при обнаружении компьютерного вируса принимает меры для «лечения» зараженного файла и удаления вируса и после этого вновь проводит антивирусный контроль.

8. В случае обнаружения на учтенном в Журнале учёта съёмных носителей персональных данных носителе вируса, не поддающегося лечению, ответственный за обеспечение безопасности персональных данных обязан:

— запретить использование носителя;
— поставить в известность ответственного за организацию обработки персональных данных;
— запретить работу в ИСПДн;
— в возможно короткие сроки обновить пакет антивирусных программ;
— провести антивирусное сканирование ИСПДн.

9. Ответственность за поддержание установленного в настоящей инструкции порядка проведения антивирусного контроля возлагается на ответственного за обеспечение безопасности персональных данных

С инструкцией ознакомлен:

_____(_____)
_____(_____)
_____(_____)
_____(_____)
_____(_____)

Приложение 2

УТВЕРЖДЕНО:
2приказом отдела культуры и искусства
администрации муниципального
образованияСтароминский район
от 27 марта 2023 года №79

Инструкция
Пользователя информационной системы персональных данных при возникновении нештатных ситуаций в отделе культуры и искусстваадминистрации МО Староминский район

1. Настоящая Инструкция определяет возможные аварийные ситуации, связанные сфункционированием информационных систем персональных данных отдела культуры и искусства администрации МО Староминский район (далее–ИСПДн), меры и средства поддержания непрерывности работы и восстановленияработоспособности ИСПДн после аварийных ситуаций.

2. Целью настоящего документа является превентивная защита элементов ИСПДн отпрерывания работоспособности в случае реализации рассматриваемых угроз.

3. Задачами данной Инструкции являются:
— определение мер защиты от прерывания работоспособности;
— определение действий по восстановлению в случае прерывания работоспособности.

4. Действие настоящей Инструкции распространяется на всех пользователей ИСПДн,имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечениянепрерывности работы и восстановления ресурсов при возникновении аварийныхситуаций, в том числе:
— системы жизнеобеспечения;
— системы обеспечения отказоустойчивости;
— системы резервного копирования и хранения данных;
— системы контроля физического доступа.

5. Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем вфункционировании элементов ИСПДн. Аварийная ситуация становится возможной врезультате реализации одной из угроз, приведенных в Приложении № 1.

6. При реагировании на инцидент важно, чтобы пользователь правильно классифицировалкритичность инцидента. Критичность оценивается на основе следующей классификации:
— Уровень 1.
Незначительный инцидент – локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств

защиты;
— Уровень 2.
Авария – любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;
— Уровень 3.
Катастрофа – любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению,блокированию, неправомерной модификации или компрометации защищаемыхперсональных данных, а также к угрозе жизни пользователей ИСПДн.

7. При возникновении нештатной ситуации любого уровня пользователь обязан оповеститьответственного за организацию обработки персональных данных, сообщив характераварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

8. Все действия в процессе реагирования на аварийные ситуации должныдокументироваться ответственным за организацию обработки персональных данных в Журнале регистрации фактов нарушения и восстановления работоспособности оборудования или ИСПДн. В кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.

9. К техническим мерам обеспечения непрерывной работы и восстановления относятсяпрограммные, аппаратные (программно-аппаратные) и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:
— системы жизнеобеспечения;
— системы обеспечения отказоустойчивости;
— системы резервного копирования и хранения данных;
— системы контроля физического доступа.
Системы жизнеобеспечения ИСПДн включают:
— пожарные сигнализации и системы пожаротушения;
— системы вентиляции и кондиционирования;
— системы резервного питания.
Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения. Порядок предотвращения потерь информации и организации восстановления ИСПДн описан в Инструкции по организации резервирования и восстановления программногообеспечения, баз персональных данных ИСПДн.

10. Ответственный за организацию обработки персональных данных:
— ознакомляет всех сотрудников, находящихся в его зоне ответственности, с даннойинструкцией в срок, не превышающий 3х рабочих дней с момента выхода новогосотрудника на работу;
— обучает пользователей, имеющих доступ к ресурсам ИСПДн, порядку действий привозникновении аварийных ситуаций.

Приложение

к Инструкции пользователя ИСПДн при возникновении нештатной ситуации

2

Источники
угроз безопасности персональных данных

Технологические угрозы:
— Пожар в здании;
— Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);
— Взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением);
— Химический выброс в атмосферу.
Внешние угрозы:
— Массовые беспорядки;
— Сбои общественного транспорта;
— Эпидемия;
— Массовое отравление персонала;
— Теракт.
Стихийные бедствия:
— Удар молнии;
— Сильный снегопад;
— Сильные морозы;
— Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушениемздания;
— Затопление водой в период паводка;
— Наводнение, вызванное проливным дождем;
— Торнадо;
— Подтопление здания (воздействие подпочвенных вод, вызванное внезапным инепредвиденным повышением уровня грунтовых вод).
ИТ-угрозы:
— Сбой системы кондиционирования в серверном помещении;
— Выход из строя файлового сервера;
— Частичная потеря информации на сервере без потери его работоспособности;
— Выход из строя локальной сети;
— Выход из строя рабочей станции;
— Частичная потеря информации на рабочей станции без потери её работоспособности.

Угроза, связанная с человеческим фактором:
— Ошибка персонала, имеющего доступ к элементам ИСПДн;

Пользователи ИСПДн должны получить базовые знания в следующих областях:
— оказание первой медицинской помощи;
— пожаротушение;

— эвакуация людей;
— защита материальных и информационных ресурсов;
— методы оперативной связи со службами спасения и руководителями структурныхподразделений;
— выключение оборудования, электричества, водоснабжения, газоснабжения;
— по окончанию ознакомления сотрудников получает их роспись в Журнале учетапрохождения первичного инструктажа.

11. Навыки и знания пользователей ИСПДн по реагированию на аварийные ситуациидолжны регулярно проверяться. При необходимости должно проводиться дополнительноеобучение пользователей ИСПДн порядку действий при возникновении аварийной ситуации. Ответственность за организацию обучения пользователей ИСПДн несет ответственный за организацию обработки персональных данныхсогласует сроки и порядок их обучения.

С инструкцией ознакомлен:

_____(_____)

_____(_____)

_____(_____)

_____(_____)

— Нарушение конфиденциальности, целостности и доступности конфиденциальной
информации, а также несанкционированные действия, заблокированные средствами

защиты и зафиксированные средствами регистрации.

Угрозы, связанные с внешними поставщиками:

— Отключение электроэнергии;
— Сбой в работе интернет-провайдера;
— Физический разрыв внешних каналов связи.

Приложение 3

УТВЕРЖДЕНО:
2приказом отдела культуры и искусства
администрации муниципального
образованияСтароминский район
от 27 марта 2023 года №79

Инструкция
пользователя информационной системы персональных данных в отделе культуры и искусства администрации муниципального образования Староминский район

1. Пользователем информационной системы персональных данных в отделе культуры и искусства администрации муниципального образования Староминский район (далее – Пользователь) является работник, осуществляющий обработкуперсональных данных в информационной системе персональных данных в отделе культуры и искусства администрации муниципального образования Староминский район (далее – ИСПДн).
Согласно ФЗ от 27.07.2006 № 152-ФЗ «О персональных данных» обработка ПДн – любоедействие (операция) или совокупность действий (операций), совершаемых сиспользованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление,уничтожение персональных данных (далее – ПДн).

2. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением обобеспечении безопасности ПДн, руководящими и нормативными документами ФСТЭК иФСБ России и внутренними нормативными актами отдела культуры и искусства администрации муниципального образования Староминский район, с которыми он былознакомлен при прохождении первичного инструктажа.

3. Пользователь несет персональную ответственность за свои действия.

4. Пользователь обязан:

— знать и выполнять требования Положения об обработке данных, Политики в отношенииобработки данных, других локальных актов оператора в отношении персональных данных;

— знать и выполнять установленные требования по режиму обработки ПДн, учету,
хранению и использованию носителей ПДн, обеспечению безопасности ПДн;

— соблюдать требования парольной политики;

Приложение 4

УТВЕРЖДЕНО:
2приказом отдела культуры и искусства
администрации муниципального
образованияСтароминский район
от 27 марта 2023 года №79

Инструкция
по учёту лиц, допущенных к работе с персональными данными в информационных системах персональных данныхотдела культуры и искусства администрации муниципального образования Староминский район

1. Настоящая инструкция определяет порядок учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных отдела культуры и искусства администрации муниципального образования Староминский район (далее – ИСПДн).

2. Порядок допуска работника к работе с персональными данными: — утверждение приказом о допуске к обработке персональных данных перечня должностей работников, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей (далее – Перечень);

— прохождение первичного инструктажа, включающего ознакомление со всеми нормативными документами, регламентирующими работу с персональными данными, согласно Инструкции по проведению инструктажа лиц, допущенных к работе с персональными данными с внесением соответствующей информации в Журнал учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными (приложение №1) в ИСПДН;

— внесение записи в Журнал учёта прав доступа к ИСПДн.

3. Допуск работника к персональным данным прекращается:

— в случае обнаружения нарушений порядка обработки персональных данных до выяснения и устранения причин нарушений;

— в случае увольнения сотрудника с момента подписания приказа об увольнении;

— при изменении его служебных обязанностей с момента утверждения нового Перечня

С инструкцией ознакомлен:

_____(_____)

_____(_____)

— блокировать АРМ в случае отсутствия на рабочем месте;
— оповещать ответственного за обеспечение безопасности ПДн о фактах нарушения информационной безопасности и возникновения нештатных ситуаций;

— при возникновении нештатных и аварийных ситуаций действовать согласно Инструкциипользователя при возникновении нештатных ситуаций с целью ликвидации их последствийи возможного ущерба.

5. Пользователю запрещается:
— разглашать обрабатываемые ПДн;
— производить несанкционированное копирование ПДн на учтенные носители;
— производить копирование ПДн на неучтенные носители;
— оставлять незаблокированным АРМ при отсутствии на рабочем месте;
— сообщать и передавать третьим лицам личные пароли и атрибуты доступа к ресурсам ИСПДн.

6. За нарушение информационной безопасности Пользователь несет ответственностьсогласно действующему законодательству Российской Федерации.

С инструкцией ознакомлен:

_____(_____)

_____(_____)

_____(_____)

_____(_____)

Приложение

2 к Инструкции по учёту лиц, допущенных к работе с персональными данными

ЖУРНАЛ УЧЁТА
учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными

№ п/п	ФИО работника	Дата прохождения инструктажа	Подпись работника	ФИО должностного лица, проводившего инструктаж	Подпись должностного лица
1	2	3	4	5	6

Приложение

2 к Инструкции по учёту лиц, допущенных к работе с персональными данными

ЖУРНАЛ УЧЁТА

учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными

№ п/п	ФИО работника	Дата прохождения инструктажа	Подпись работника	ФИО должностного лица, проводившего инструктаж	Подпись должностного лица
1	2	3	4	5	6

Приложение 5

УТВЕРЖДЕНО:
приказом муниципального бюджетного учреждения культуры «Староминский историко-краеведческого музея» муниципального образования Староминский район
от 23 мая 2023 года № 78

Инструкция
по учёту и хранению съёмных носителей персональных данных в отделе культуры и искусства администрации муниципального образования Староминский район

1. Общие положения

1.1. Настоящая «Инструкция по учёту и хранению съёмных носителей персональныхданных» (далее — Инструкция) определяет порядок работы со съёмными носителямиперсональных данных в отделе культуры и искусства администрации муниципального образования Староминский район" (далее — Оператор) в соответствии с Федеральнымзаконом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлениемПравительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защитеперсональных данных при их обработке в информационных системах персональных данных», иными нормативными правовыми актами РФ в области защиты персональныхданных.

1.2. С Инструкцией знакомятся под подпись и выполняют её все лица, допущенные кобработке персональных данных «Приказом о допуске к обработке персональных данных».

2. Определения

Съёмный носитель персональных данных — носитель информации, используемый дляхранения и передачи персональных данных в электронной форме.

Пользователь — работник Оператора или сотрудник по договору гражданско-правовогохарактера, допущенный к обработке персональных данных «Приказом о допуске кобработке персональных данных».

3. Порядок работы со съёмными носителями

3.1. Ответственный за обеспечение безопасности персональных данных, либоуполномоченный им работник, выдаёт съёмные носители пользователям только в случаяхпроизводственной необходимости.

3.2. Все съёмные носители персональных данных учитываются и выдаются пользователямпод подпись.

3.3. Пользователям, получившим съёмные носители персональных данных под подпись,запрещается передавать их третьим лицам.

3.4. Ответственный за обеспечение безопасности персональных данных, либоуполномоченный им работник, изымает съёмные носители персональных данных приувольнении пользователя.

3.5. Все съёмные носители персональных данных хранятся в запираемых шкафах илисейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чемдвумя дубликатами ключей).

3.6. Допускается хранение съёмных носителей персональных данных вне запираемых
шкафов или сейфов (металлических шкафов) при условиях уничтожения персональныхданных в соответствии с Инструкцией по порядку уничтожения и обезличиванияперсональных данных, либо если на съёмном носителе персональных данных хранятся
только персональные данные в зашифрованном или обезличенном виде.

3.7. Право на перемещение съёмных носителей информации за пределы территории, накоторой осуществляется обработка, имеют только те лица, которым это необходимо длявыполнения своих должностных обязанностей.

3.8. Использование неучтённых съёмных носителей для обработки персональных данныхфиксируется как несанкционированное, а ответственный за обеспечение безопасностиперсональных данных инициирует служебную проверку. По факту выясненныхобстоятельств составляется Акт проведения расследования инцидента.

3.9. Пользователи, в случаях утраты или кражи съёмных носителей персональных данных,сообщают об этом ответственному за обеспечение безопасности персональных данных.

3.10. Съёмные носители персональных данных, пришедшие в негодность, или отслужившиев установленный срок, подлежат уничтожению в соответствии с Инструкцией по порядкууничтожения и обезличивания персональных данных. По результатам уничтожениясоставляется Акт уничтожения персональных данных.

4. Порядок организации учёта съёмных носителей

4.1. На каждом съёмном носителе персональных данных размещается этикетка суникальным учётным номером.

4.2. Ответственный за обеспечение безопасности персональных данных, либоуполномоченный им работник, при выдаче, приёме, уничтожении съёмных носителейперсональных данных вносит в Журнал учета съёмных носителей персональных данных(Приложение 1):
— учётный номер, размещённый на этикетке на съёмном носителе персональных данных;

— тип съёмного носителя (USB-накопитель, внешний жёсткий диск, CD/DVD диск);
— серийный или инвентарный номер съёмного носителя;
— место хранения (номер запираемого шкафа или сейфа, номер помещения);
— дату и номер Акта уничтожения персональных данных в случае уничтожения съёмногоносителя;
— подпись.

4.3. Пользователи при получении либо сдаче съёмных носителей персональных данныхзаносят в Журнал учёта съёмных носителей персональных данных свои фамилию, имя, отчество, ставят дату и подпись.

5. Ответственность

5.1. Все работники Оператора, допущенные в установленном порядке к работе сперсональными данными, несут административную, материальную, уголовнуюответственность в соответствии с действующим законодательством за обеспечениесохранности и соблюдению правил работы с персональными данными.

5.2. Ответственность за доведение требований настоящей Инструкции до работниковОператора несёт ответственный за организацию обработки персональных данных.

5.3. Ответственность за обеспечение мероприятий по реализации требований настоящейИнструкции, в том числе учёт, выдачу, уничтожение съёмных носителей персональныхданных несёт ответственный за обеспечение безопасности персональных данных.

С инструкцией ознакомлен:

_____(_____)
_____(_____)
_____(_____)
_____(_____)

Приложение

к Инструкции по учёту и хранению съёмных носителей

ЖУРНАЛ УЧЁТА
съёмных носителей персональных данных

п/п	Учётный номер	Тип носителя	Номер (серийный/ инвентарный)	Место хранения	Расписка в получении		Дата и номер акта уничтожения	Подпись ответственного лица	Примечание
					Ф.И.О. Дата получения носителя	Ф.И.О. Дата сдачи носителя			
1	2	3	4	5	6	7	8	9	10

Приложение 6

УТВЕРЖДЕНО:
приказом муниципального бюджетного учреждения культуры «Староминский историко-краеведческого музея» муниципального образования Староминский район
от 23 мая 2023 года № 78

Инструкция
по порядку уничтожения и обезличивания персональных данных в ИСПДн отделе культуры и искусства администрации муниципального образования Староминский район

1. Общие положения

1.1. Настоящая инструкция определяет порядок уничтожения и обезличиванияинформации, содержащей персональные данные, при достижении целей обработки или принаступлении иных законных оснований в отделе культуры и искусства администрации муниципального образования Староминский район (далее — Оператор).

1.2. Инструкция разработана в соответствии с ч. 7 ст. 5, ч. 4 ст. 21 и п. 9 ч. 1 ст. 6Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «Оперсональных данных»), «Требованиями и методами по обезличиванию персональныхданных, обрабатываемых в информационных системах персональных данных, в том числесозданных и функционирующих в рамках реализации федеральных целевых программ», утверждёнными приказом Федеральной службы по надзору в сфере связи,информационных технологий и массовых коммуникаций от 5 сентября 2013 г. № 996 иными нормативными правовыми актами РФ в области защиты персональных данных.

2. Условия и порядок уничтожения информации, содержащей персональные данные

2.1. Оператор уничтожает информацию, содержащую персональные данные:
— по достижении целей обработки или в случае утраты необходимости в достижении этихцелей;
— по достижении окончания срока хранения;
— при наступлении иных законных оснований.

2.2. Уничтожение информации, содержащей персональные данные, производится в случае
достижения цели обработки в срок, не превышающий тридцати дней с даты достижения

цели обработки персональных данных.

2.3. Уничтожение информации, содержащей персональные данные, производится в случае

выявления неправомерной обработки в срок, не превышающий десяти дней с моментавыявления неправомерной обработки персональных данных.

2.4. Решение об уничтожении ПД принимается комиссией по уничтожению носителей, содержащих персональные данные, положение о комиссии и ее состав утверждается приказом отдела.

Акт об уничтожении носителей, содержащих ПД субъектов ПД, составляется по установленной форме (Приложение 1),акт об уничтожении ПД в электронной форме (приложение 2).

2.5. К персональным данным, хранимым в электронном виде, относятся файлы, папки, электронные архивы на жестком диске компьютера и съёмных машинных носителях(компакт-дисках CD-R/RW или DVD-R/RW, дискетах 3,5, флеш-носителях).

2.6. Съёмные машинные носители по истечению сроков обработки и хранения на нихперсональных данных подлежат уничтожению с целью невозможности восстановления идальнейшего использования. Это достигается путем деформирования, нарушения единойцелостности носителя или его сжигания.

2.7. В случае допустимости повторного использования съёмного машинного носителяприменяется программное удаление («затирание») содержимого путём его форматированияс последующей записью новой информации на данный носитель.

2.8. Подлежащие уничтожению файлы с персональными данными, расположенные нажестком диске информационной системы персональных данных, удаляются средствамиоперационной системы компьютера с последующим «очищением корзины».

2.9. Черновики документов, испорченные листы, варианты и неподписанные проектыдокументов уничтожаются путём их сожжения или измельчения или другим путем, исключающим восстановление текста документов.

3. Условия и порядок обезличивания информации, содержащей персональные данные

3.1. Оператор может обезличивать персональные данные в статистических или иныхисследовательских целях, по достижении целей обработки персональных данных или вслучае утраты необходимости в достижении этих целей, если иное не предусмотренофедеральным законом.

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

— замена части данных идентификаторами;

— обобщение, изменение или удаление части данных;

— деление данных на части и обработка в разных информационных системах;

— перемешивание данных;
— другие способы.

3.3. В случае достижения целей обработки персональных данных или в случае утратынеобходимости в достижении этих целей способом обезличивания является уменьшениеперечня обрабатываемых данных.

3.4. Ответственный за организацию обработки персональных данных назначаетсяответственным за проведение мероприятий по обезличиванию персональных данных.

3.5. Решение о необходимости обезличивания персональных данных и способ обезличивания принимает ответственный за организацию обработки персональныхданных.

3.6. Обезличенные персональные данные не подлежат разглашению и нарушениюконфиденциальности.

3.7. Обезличенные персональные данные могут обрабатываться с использованием и безиспользования средств автоматизации.

3.8. При использовании процедуры обезличивания не допускается совместное хранениеперсональных данных и обезличенных данных.

3.9. В процессе обработки обезличенных данных, при необходимости, может производиться де обезличивание. После обработки персональные данные, полученные в результате такого де обезличивания, уничтожаются.

3.10. Обработка персональных данных до осуществления процедур обезличивания и после выполнения операций де обезличивания должна осуществляться в соответствии сзаконодательством Российской Федерации с применением мер по обеспечениюбезопасности персональных данных

4. Ответственность

4.1. Ответственность за осуществление контроля выполнения требований настоящейинструкции несет ответственный за организацию обработки персональных данныхОператора.

4.2. Ответственность за выполнение настоящей инструкции возлагается на ответственногоза организацию обработки персональных данных, ответственного за обеспечениебезопасности персональных данных и всех работников Оператора, допущенных к обработкеобезличенных персональных данных, в соответствии с действующим законодательством.

С инструкцией ознакомлен:

_____(_____)

_____(_____)

_____(_____)

_____(_____)

Приложение 1

к Инструкции по порядку
уничтожениями обезличивания
персональных данных

Утверждаю
Начальник отдела культуры
и искусства администрации
муниципального образования
Староминский район_____ Ф.И.О.
«____»_____202__года

Акт
об уничтожении персональных данных сотрудников

ст.Староминская _____ 202___ года

Комиссия в составе:
председателя комиссии: _____
секретаря комиссии: _____
членов комиссии:
_____
_____
составила настоящий акт о том, что _____202__ года с помощью
_____
(указать способ уничтожения шредер или сжигание)

в присутствии комиссии были уничтожены персональные данные работников отдела культуры и искусства администрации муниципального образования Староминский район в следующем объеме:

№ п/п	*Вид материального носителя персональных данных*	*Дата уничтожения*	*Процедура уничтожения материального носителя*	*Причина уничтожения материального носителя персональных данных*

ИТОГО:

Возможность дальнейшего использования персональных данных или их восстановления исключена. Данный факт подтверждает комиссия в составе:

Председателя комиссии: _____
Секретаря комиссии: _____
Членов комиссии:

_____
_____

Настоящий акт составлен в двух экземплярах:
первый экземпляр — у председателя комиссии;
второй экземпляр — подшит в дело № _____.

Ответственный за
организацию обработки
персональных данных

Приложение 2

к Инструкции по порядку
уничтожениями обезличивания
персональных данных

Утверждаю
Начальник отдела культуры
и искусства администрации
муниципального образования
Староминский район_____ Ф.И.О.
«____»_____202__года

Акт
об уничтожении персональных данных сотрудников хранящихся в информационной системе персональных данных

ст. Староминская _____ 202___ года

Комиссия в составе:
председателя комиссии: _____
секретаря комиссии: _____
членов комиссии:
_____
_____
составила настоящий акт о том, что в связи с истечением сроков обработки персональных данных, хранящихся в информационных системах персональных данных (ИСПДн), произведено их уничтожение (удаление):

№	ИСПДн	Объем данных	Период	Примечание

Председатель комиссии: _____
Секретарь комиссии: _____
Членов комиссии:
_____
_____

Приложение 7

УТВЕРЖДЕНО:
приказом муниципального бюджетного учреждения культуры «Староминский историко-краеведческого музея» муниципального образования Староминский район
от 23 мая 2023 года № 78

Инструкция
по проведению инструктажа лиц, допущенных к работе с информационной системой персональных данных отдела культуры и искусства администрации муниципального образования Староминский район

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных отдела культуры и искусства администрации муниципального образования Староминский район (далее – ИСПДн).

2. При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к ИСПДн (далее – новый сотрудник), ответственный за организацию обработки персональных данных:

1) в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и локальными актами организации в отношении обработки персональных данных, перечисленными в Приложении 1 к данной инструкции;

2) знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;

3) отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.

3. Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

Приложение 1

к Инструкции по проведению
инструктажа лиц, допущенных к работе с
информационными системами
персональных данных

Перечень
законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа

Законодательные акты Российской Федерации о персональных данных:

1) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.07.2014).

2) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные, в том числе без использования средств автоматизации).

3) Трудовой кодекс Российской Федерации от 30.12.2001 г. № 197-ФЗ - Глава 14 «Защита персональных данных работника»

4) Федеральный закон от 21.07.2014 г. № 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях";

5) Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

6) Указ Президента Российской Федерации от 30.05.2005 г. № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»;

7) Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-РП «О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных»;

8) Постановление Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

9) Постановление Правительства Российской Федерации от 03.11.1994 г. № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использования атомной энергии и уполномоченном органе по космической деятельности»;

10) Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

11) Постановление Правительства Российской Федерации от 06.07.2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

12) Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

13) Приказ Роскомнадзора от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

14) Распоряжение Правительства Российской Федерации от 15.08.2007 г. № 1055-Р «О плане подготовки проектов нормативных актов, необходимых для реализации Федерального закона «О персональных данных»

15) Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

16) Приказ Роскомнадзора от 30.10. 2018 г. № 159 "О внесении изменений в Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 мая 2017 года № 94";

17)Постановление Правительства Российской Федерации от 13.02.2019 № 146 "Об утверждении Правил организации и осуществления государственного контроля и надзора за обработкой персональных данных".

Внутренние локальные акты отдела культуры и искусства администрации муниципального образования Староминский район:

1) Приказ о допуске к обработке персональных данных.

2) Политика в отношении обработки персональных данных.

3) Положение об обработке персональных данных.

4) Правила о порядке доступа в помещения, в которых ведётся обработка персональных данных.

5) Положение об обработке персональных данных без использования средств автоматизации.

6) Инструкция по учёту и хранению съёмных носителей персональных данных.

7) Инструкция по организации резервного копирования и восстановления в ИСПДн.

8) Инструкция по антивирусной защите.

9) Инструкция по проведению инструктажа лиц, допущенных к работе с ПДн.

10) Инструкция по проведению внутреннего контроля.

11) Инструкция по порядку уничтожения и обезличивания персональных данных.

12) Инструкция пользователя ИСПДн.

13) Инструкция пользователя при возникновении нештатной ситуации.

14) План проведения внутреннего контроля.

15)Положение о порядке доступа в помещения, в которых ведется обработка ПДн.

16) Положение о порядке хранения и защиты персональных данных пользователей в отделе культуры и искусства администрации муниципальногообразованияСтароминский **район**;

17)Регламент допуска работников к обработке персональных данных;

18)Положение об уничтожении и обезличивании персональных данных;

19)Формы документов необходимых для выполнения требований законодательства в области персональных данных в отделе культуры и искусства администрации муниципального образования Староминский район;

20)Правила оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности персональных данных

С инструкцией ознакомлен:

_____(_____)

_____(_____)

_____(_____)

_____(_____)

Приложение 8

УТВЕРЖДЕНО:
приказом муниципального бюджетного учреждения культуры «Староминский историко-краеведческого музея» муниципального образования Староминский район
от 23 мая 2023 года № 78

Инструкция
по проведению внутреннего контроля
соответствия обработки персональных данных требованиям
к защите персональных данных в отделе культуры и искусства
администрации муниципального образования Староминскийрайон

1. Общие положения

1.1. Настоящая «Инструкция по проведению внутреннего контроля соответствия обработкиперсональных данных требованиям к защите персональных данных» (далее — Инструкция) определяет порядок осуществления внутреннего контроля соответствия обработкиперсональных данных требованиям к защите персональных данных в отделе культуры и искусства администрации муниципального образования Староминский район (далее— Оператор) в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «Оперсональных данных», иными нормативными правовыми актами РФ в области защитыперсональных данных.

1.2. Инструкцию обязаны выполнять все работники Оператора, допущенные к обработкеперсональных данных «Приказом о допуске к обработке персональных данных».

2. Порядок проведения внутреннего контроля

2.1. В целях осуществления внутреннего контроля соответствия обработки персональныхданных установленным требованиям Оператор организует проведение периодическихпроверок условий обработки персональных данных.

2.2. Внутренний контроль проводит ответственный за организацию обработкиперсональных данных (далее — Ответственный).

2.3. Внутренний контроль осуществляется не реже 1 раза в 3 года. При необходимостиконтроль может проводиться чаще в соответствии с поручением Оператора.

2.4. Ответственный проводит внутренний контроль непосредственно на месте обработки персональных данных, опрашивает работников, осуществляющихобработку персональных данных, осматривает рабочие

места. Все работники обязаны позапросу контролирующих предъявить все материалы и документы, числящиеся за ними, дать устные или письменные объяснения по существу заданных вопросов.

2.5. По результатам проверки составляется Акт контроля соответствия обработкиперсональных данных по форме, приведённой в Приложении 1.

2.6. При выявлении нарушений в ходе проверки Ответственным:

- делается запись в Акте контроля соответствия обработки персональных данных омероприятиях по устранению нарушений и сроках их исполнения;

- информация о нарушениях и о мерах для их устранения доводится до сведенияруководителя организации.

2.7. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть 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 до ввода в эксплуатацию информационной системы 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.

2.8. В ходе внутренней проверки контролирующие проводят:

— контроль соответствия обработки персональных данных требованиям законодательства,нормативных актов по вопросам обработки персональных данных;

— контроль выполнения организационных и технических мер по обеспечениюбезопасности персональных данных при их обработке;

— проверку параметров настройки и правильности функционирования программногообеспечения и средств защиты информации;

— анализ изменения угроз безопасности персональных данных в информационной системе Оператора, возникающих в ходе её эксплуатации;

— контроль наличия или отсутствия фактов несанкционированного доступа к персональным данным;

— контроль соблюдения работниками, допущенными к обработке

персональных данных, «Положения об обработке персональных данных», «Инструкции по порядку уничтожения иобезличивания персональных данных», «Инструкции по учёту и хранению съёмных носителей персональных данных», «Положения о порядке доступа в помещения» и других локальных актов, регламентирующих обработку персональных данных Оператора;

— проверку «Журнала учёта съёмных носителей персональных данных».

3. Ответственность

3.1. За организацию проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства отвечает Ответственный.

3.2. Ответственность за соблюдение Инструкции возлагается на всех работников Оператора, на которых распространяется Инструкция.

С инструкцией ознакомлен:

_____(_____)

_____(_____)

_____(_____)

_____(_____)

Приложение 1

Инструкции по проведению
внутреннего контроля
соответствия обработки
персональных данных
требованиям к защите персональных
данных

АКТ
контроля соответствия обработки персональных данных

В соответствии с п. 4 ч. 1 ст. 18.1 Федерального закона от 27 июля 2006 г. № 152-ФЗ «Оперсональных данных» вотделе культуры и искусстваадминистрации МО Староминский район (далее — Оператор) проведен контрольсоответствия обработки персональных данных следующим актам:

— Федеральному закону от 27июля 2006 г. № 152-ФЗ «О персональных данных» и принятымв соответствии с ним нормативным правовым актам, требованиям к защите персональныхданных, в том числе «Положению об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждённомупостановлением Правительства от 15 сентября 2008 г. № 687, и «Требованиям к защите персональных данных при их обработке в информационных системах персональныхданных», утверждённым постановлением Правительства от 1 ноября 2012 г. № 1119;

— Политике в отношении обработки персональных данных;

— Положению об обработке персональных данных;

— иным локальным актам.

В результате проведения контроля.,выявлены нарушения:

_____

_____

Меры по устранению нарушений:

_____

_____

Срок устранения нарушений:

_____

_____

Ответственный за
организацию обработки
персональных данных_____

Приложение 1

Инструкции по проведению
внутреннего контроля
соответствия обработки
персональных данных
требованиям к защите персональных
данных

План проведения
периодического внутреннего контроля условий обработки персональных данных в ИСПДн отдела культуры и искусства
администрации МО Староминский район

Общие положения

1. Периодический внутренний контроль соответствия обработки и защиты персональныхданных установленным требованиям (далее – внутренний контроль) в информационныхсистемах персональных данных отдела культуры и искусстваадминистрации МО Староминский район (далее – ИСПДн) проводится в целяхвыполнения требований п. 4 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «Оперсональных данных».

2. Внутренний контроль:

— осуществляется в соответствии с Инструкцией по проведению внутреннего контролясоответствия обработки персональных данных требованиям к защите персональныхданных;

— проводится Ответственным за организацию обработки персональных данных.

3. План проведения внутреннего контроля содержит следующую информацию:

— название мероприятия;

— период проведения контроля.

4. По результатам проведения внутреннего контроля оформляется Акт контролясоответствия обработки персональных данных.

5. Начальник отдела культуры определяет сроки внутреннего контроля, но нереже 1 раза в 3 года.

План
проведения внутреннего контроля

№ п/п	Мероприятие	Дата
1	Проверка полноты, качества и актуальности разработанных внутреннихраспорядительных и нормативно-методических документов, регламентирующих обработку и обеспечение безопасности ПДн	
2	Контроль выполнения требований по режиму доступа в здание,помещения и на автоматизированные рабочие места, где ведетсяобработка ПДн	
3	Проверка порядка использования технических средств защиты ПДн	
4	Проверка выполнения требований действующих нормативныхдокументов по защите персональных данных	
5	Проверка и выявления изменений в режиме обработки ПДн	
6	Анализ и пересмотр имеющихся угроз безопасности ПДн, выявление новых угроз	
7	Проверка актуальности сведений в Реестре операторов персональныхданных Роскомнадзора (если организация включена в Реестр)	
8	Подведение итогов	
9	Устранение недостатков	
10	Составление акта внутреннего контроля	
11	Отчёт о проведении проверки	

Приложение 9

УТВЕРЖДЕНО:
приказом муниципального бюджетного учреждения культуры «Староминский историко-краеведческого музея» муниципального образования Староминский район
от 23 мая 2023 года № 78

Инструкция
по организации резервирования
и восстановления программного обеспечения,
баз персональных данных информационной системы
персональных данных в отделе культуры и искусства администрации
муниципального образования Староминский район

1. Настоящая инструкция разработана с целью обеспечения возможностинезамедлительного восстановления персональных данных в информационной системеперсональных данных, модифицированных или уничтоженных вследствиенесанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядоквосстановления работоспособности информационной системы персональных данных отделе культуры и искусства администрации муниципального образования Староминский район.

2. Резервированию подлежат базы данных и файлы, содержащие персональные данные.

3. Резервирование выполняется штатным средством архивирования системы и данных«ntbackup» и производится на локальный дисковый массив. Процедура резервногокопирования производится каждый день.

4. Ответственным за процедуру резервирования и восстановления назначаетсяответственный за организацию обработки персональных данных.

5. Восстановление файлов производится путем разархивирования файлов базы данных висходный каталог.

С инструкцией ознакомлен:

_____(_____)
_____(_____)
_____(_____)
_____(_____)

Приложение 10

УТВЕРЖДЕНО:
приказом муниципального бюджетного учреждения культуры «Староминский историко-краеведческого музея» муниципального образования Староминский район
от 23 мая 2023 года № 78

Инструкция

ответственного за организацию обработки персональных данных в отделе культуры и искусства администрации муниципального образования Староминский район

1. Общие положения

Должностная инструкция ответственного за организацию обработки персональных данных (далее – Инструкция) в отделе культуры и искусства администрации муниципального образования Староминский район (далее – отдел культуры) определяет ответственность, права и обязанности ответственного за организацию обработки персональных данных в отделе культуры.

1.1. Инструкция разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Ответственный назначается на должность из числа штатных сотрудников приказом начальника отдел культуры.

1.3. На время отсутствия Ответственного его обязанности исполняет начальник отдела культуры, который приобретает соответствующие права и несет ответственность за надлежащее исполнение возложенных на него обязанностей.

1.4. Ответственный в своей работе руководствуется:

- федеральными и региональными ннормативными правовыми актами, регулирующими вопросы в области обеспечения безопасности персональных данных;
- методическими материалами по вопросам защиты информации;
- приказами отдел культуры;
- настоящей Инструкцией.

2. Должностные обязанности

Ответственный должен:

2.1. Знать и соблюдать требования действующего законодательства Российской Федерации в области персональных данных и защиты информации, порядок систематизации, учета и ведения документации, в том числе с использованием современных информационных технологий, правила и нормы охраны труда.

2.2. Осуществлять контроль соблюдения в отделе культуры законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных и правил их обработки.

2.3. Проводить периодические проверки соответствия обработки персональных данных установленным требованиям в отделе культуры.

2.4. Доводить до сведения, разъяснять работникам отдела культуры положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.5. Проводить инструктажи и занятия по изучению правовой базы по защите персональных данных с сотрудниками отдела культуры, имеющими доступ к персональным данным, и вести Журнал проведения инструктажей по информационной безопасности.

2.6. Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений правил обработки персональных данных.

2.7. Не допускать к работе с персональными данными лиц, не обладающих для этого соответствующими правами.

2.8. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.9. Осуществлять методическое руководство работой администраторов безопасности и администраторов информационных систем персональных данных отдела культуры в области защиты персональных данных.

3. Права работника

Ответственный имеет право:

3.1. Требовать от сотрудников отдела культуры соблюдения законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, правил их обработки и других нормативных документов в области обработки и защиты персональных данных.

3.2. Знакомиться с проектами решений начальника отдела культуры, касающимися его деятельности.

3.3. Вносить на рассмотрение начальника отдела культуры предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей Инструкцией.

3.4. Подписывать и визировать документы в пределах своей компетенции.

3.5. Осуществлять взаимодействие с руководителями учреждений культуры муниципального образования Староминский район, получать информацию и документы, необходимые для выполнения своих должностных обязанностей.

3.6. Повышать свою профессиональную квалификацию.

3.7. Требовать организованное рабочее место, соответствующее нормам охраны труда.

3.8. Требовать соответствия нормам Трудового Законодательства.

4. Ответственность работника

Работник несет ответственность:

4.1. За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, в пределах, определенных трудовым законодательством Российской Федерации.

4.2. За причинение материального ущерба работодателю, в пределах, определенных действующим трудовым, уголовным и гражданским законодательством Российской Федерации.

4.3. За совершенные в процессе осуществления своей деятельности правонарушения в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

С инструкцией ознакомлен:

_____(_____)
_____(_____)
_____(_____)
_____(_____)

Приложение 11

УТВЕРЖДЕНО:
приказом муниципального бюджетного учреждения культуры «Староминский историко-краеведческого музея» муниципального образования Староминский район
от 23 мая 2023 года № 78

Инструкция
пользователя информационной системы персональных данных

1. Общие положения

1.1. Настоящая Инструкция пользователя информационных систем персональных данных отдела культуры и искусства администрации муниципального образования Староминский район (далее – Инструкция/Отдел) определяет общие правила работы работников в информационных системах персональных данных Отдела.

1.2. В настоящей Инструкции применяются следующие термины и определения:

Персональные данные (ПДн)– любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или

автоматизированными системами.

Посторонние лица – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права самостоятельного доступа в информационные системы и (или) не имеют допуска к защищаемой информации.

Средство защиты информации от несанкционированного доступа (СЗИ НСД) – программное, техническое или программнотехническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных Отдела.

1.3. Пользователем является каждый работник Отдела, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обработке персональных данных Отдела и локальными нормативными актами, регламентирующими обработку персональных данных.

2. Обязанности пользователя

2.1. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов Отдела, регламентирующих порядок обработки персональных данных.

2.2. Выполнять на автоматизированном рабочем месте (персональный компьютер или терминал, далее - АРМ) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

2.4. Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных Отдела.

2.5. Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

2.6. Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя.

2.7. Незамедлительно, в кратчайшие сроки, сообщать

непосредственному руководителю об утрате или недостаче носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению персональных данных.

2.8. При прекращении работ (трудовых отношений) все материальные носители, содержащие персональные данные (флэш-накопители, дискеты, компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, и пр.), передать начальнику.

2.9. Использовать информационные ресурсы Отдела и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.

2.10. Соблюдать требования парольной политики (раздел 3 настоящей Инструкции).

2.11. Соблюдать требования антивирусной защиты (раздел 4 настоящей Инструкции).

2.12. Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена – Интернет (раздел 5 настоящей Инструкции).

2.13. Пользователи, работающие с персональными данными контрагентов организации, все наработанные файлы должны хранить на определенном Администратором сетевом диске/папке.

2.14. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.15. Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а также для получений консультаций по вопросам обработки персональных данных необходимо обращаться к Администратору ИСПДн или ответственному за организацию обработки персональных данных.

2.16. Пользователям запрещается:

2.16.1. Нарушать установленные в Отделе правила обработки персональных данных.

2.16.2. Использовать компоненты программного и аппаратного обеспечения Отдела в неслужебных целях.

2.16.3. Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы Windows или Linux – комбинацией клавиш [WIN] + [L] или [CTRL] + [ALT] + [DEL] с дальнейшим нажатием кнопки «Блокировка» появившегося меню, либо при помощи штатных средств защиты информации от несанкционированного доступа при их наличии).

2.16.4. Оставлять без присмотра или неубранными в хранилища (шкаф,

сейф) носители или документы, содержащие персональные данные.

2.16.5. Записывать и хранить конфиденциальную информацию (в том числе персональные данные) на неучтенных носителях информации (оптических (CD) дисках, гибких магнитных дисках, флеш-накопителях и т.п.).

2.16.6. Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

2.16.7 Самостоятельно разрабатывать или использовать нерегламентированные (без разрешения непосредственного руководителя, не относящиеся к производственному процессу) программы (например, игры; IM-клиенты, такие как Google Messenger, Microsoft Messenger, ICQ и т.п.; P2Pклиенты: Kazaa, eMule, Skype и т.п.).

2.16.8. Разрешать посторонним лицам работать под своей учетной записью на АРМ.

2.16.9. Пересылать конфиденциальную информацию, в том числе персональные данные, по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования или шифрования и электронной подписи).

2.16.10. Получать доступ к сети Интернет любыми способами, кроме как установленными настоящей Инструкцией, например, при помощи несанкционированно установленных на АРМ модемов и т. п.

2.16.11. Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

2.16.12. В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

2.16.13.. Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

2.16.14. Удалять или искажать программы и файлы с конфиденциальной информацией, в том числе персональных данных, и иной важной информацией (например, системной, необходимой для функционирования информационных систем).

2.16.15. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению внештатной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения и сотрудников, ответственных за установку и (или) сопровождение программного обеспечения.

2.16.16. Подключать к ЛВС Отдела личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а также личные носители и накопители информации. В случае необходимости переноса информации с личных носителей информации обращаться к

системному администратору.

3. Парольная политика

3.1. Общие требования к паролям:

3.1.1. Минимальное требование: буквенно-цифровой пароль. Желательно использовать буквы в верхнем или нижнем регистрах, цифры или специальные символы (например, ~ ! @ # $ % ^ & * ( ) _ - + = | \ ? / . , : ; '] [{ } < > . и т.п.).

3.1.2. Минимальная длина пароля: не менее 8-ми (восьми) символов.

3.1.3. Максимальный срок действия пароля: 180 суток.

3.1.4. Запрет использования трех ранее использовавшихся паролей.

3.1.5. Пароль пользователя не должен включать в себя легко вычисляемые сочетания символов, общепринятые сокращения, имена, фамилии, должности, год рождения, номер паспорта, табельный номер, иную информацию о Пользователе, доступную другим лицам.

3.1.6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

3.1.7. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567, qwerty и т.п.).

3.2. Правила использования паролей:

3.2.1. Хранить в тайне свой пароль, не сообщать его другим лицам.

3.2.2. Не давать доступ в информационные системы другим лицам под своей учетной записью и паролем.

3.2.3. Изменять свой пароль при первом требовании политики паролей операционной системы (информационной системы).

3.2.4. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.2.5. Немедленно сообщить ответственному по парольной защите об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3.2.6. Запрещается записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.

3.2.7. Запрещается хранить пароли в записанном виде на отдельных листах бумаги.

3.2.8. Смена, удаление личного пароля любого Пользователя производится в следующих случаях:

– в случае подозрения на компрометацию пароля;

– по окончании срока действия;

– в случае прекращения полномочий (увольнение, переход на другую

работу внутри Отдела)

3.2.9. При увольнении, переходе на новую должность работника, имеющего доступ помимо своей учетной записи к другим ресурсам (межсетевые экраны, маршрутизаторы, серверы, другие учетные записи и т.п.) также производится внеплановая смена паролей к таким ресурсам.

4. Антивирусная защита

4.1. В случае отсутствия штатных функций антивирусной программы, предусматривающих автоматическую проверку файлов, Пользователь обязан осуществлять проверку файлов, получаемых:

– по электронной почте;

– через сеть Интернет;

– на магнитном, оптическом диске, флэш–накопителе;

– ином съемном носителе информации;

– полученные иным способом.

4.2. Пользователю запрещается:

4.2.1. Осуществлять действия, направленные на выключение антивирусной программы;

4.2.2. Самостоятельно устанавливать на АРМ программное обеспечение;

4.2.3. Запускать файлы, полученные по сетям связи (электронной почте, Интернет), со съемных носителей, даже если они получены проверенного адресата, без предварительной их проверки антивирусной программой.

4.3. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь самостоятельно или вместе с ответственным за антивирусную защиту должен провести внеочередной антивирусный контроль своего рабочего места.

4.4. В случае обнаружения при проведении антивирусной проверки вирусного заражения Пользователи обязаны:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения вирусного заражения ответственного за антивирусную защиту;

– совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

– провести лечение или уничтожение зараженных файлов .

5. Порядок работы в информационных системах и сети интернет

5.1. Подключение к информационным системам и сервисам сети Интернет.

5.1.1. Целью работы Пользователя в информационных системах и сети Интернет является сбор, обработка, хранение общедоступной и служебной информации, обмен электронными сообщениями в служебных целях.

5.1.2. Доступ к ресурсам информационных систем и сервисам сети Интернет предоставляется Пользователям только в том случае, если это не противоречит требованиям по защите информации (требованиям настоящей Инструкции и иных нормативных документов в области защиты информации).

5.1.3. Возможность получить доступ к ресурсам информационных систем и сервисам сети Интернет не является гарантией того, что запрошенный ресурс или сервис является разрешенным.

5.1.4. Основанием для подключения работника Отдела к ресурсам информационных систем и сервисам сети Интернет является мотивированная заявка Администратору от непосредственного руководителя Пользователя с указанием полномочий доступа к таким ресурсам и сервисам.

5.1.5.Работник организует подключение к сервисам сети Интернет в установленном порядке.

5.1.6. Основанием для отключения от информационных систем и сервисов сети Интернет являются следующие события:

– нарушение инструкций и иных локальных нормативных актов в области защиты информации Университета;

– в случае нарушения Пользователем действующего законодательства в сфере компьютерной информации;

– увольнение Пользователя.

5.2. Порядок работы в сети Интернет.

5.2.1. Использование сотрудниками Отдела сети Интернет должно осуществляться исключительно для выполнения должностных обязанностей.

5.2.2. Информация, образованная (образующаяся) в процессе трудовой деятельности работника, является собственностью Отдела и не подлежит использованию, в том числе использованию в сети Интернет или с помощью сети Интернет в личных целях и (или) в корыстных интересах других лиц (организаций).

5.2.3. При проведении технических работ, связанных с настройкой оборудования (коммуникационное оборудование, прокси-сервера, маршрутизаторы и т.п.); в случае обнаружения попыток несанкционированного доступа к Интернет-шлюзу, может проводиться временное отключение Пользователей от сервисов сети Интернет (в случае планового отключения Пользователи уведомляются об этом заблаговременно).

5.2.4. При работе в сети Интернет запрещается:

– умышленное распространение и получение материалов в/из сети Интернет, противоречащих законодательству Российской Федерации, в том числе материалов, пропагандирующих насилие или экстремизм; разжигающих расовую, национальную или религиозную вражду;

разъясняющих порядок изготовления и/или применения наркотиков, взрывчатых веществ, оружия и т. п.; материалов порнографического характера; компьютерных вирусов и других вредоносных программ;

– передавать в сеть Интернет информацию, к которой в соответствии с законодательством ограничен доступ (персональные данные, коммерческая тайна) без соответствующего разрешения;

– фальсифицировать IP-адрес, MAC-адрес, иные адреса, используемые в сетевых протоколах, а также прочую служебную информацию при передаче данных через сеть Интернет.

– предоставлять доступ в сеть Интернет со своей рабочей станции;

– получать доступ к сети Интернет любыми способами, не предусмотренными действующими локальными нормативными актами Отдела (инструкциями, положениями, регламентами);

– осуществлять несанкционированный доступ к ресурсам и сервисам сети Интернет.

– выполнять действия (взлом, DoS (отказ в обслуживании), ARPspoofing атаки, сканирование локальной вычислительной сети) направленные на нарушение функционирования элементов сети Интернет (коммуникационного оборудования, серверов, рабочих станций, программного обеспечения).

5.3. Правила работы Пользователей с электронной почтой:

5.3.1. Пользователи обязаны использовать электронную почту только для выполнения служебных обязанностей.

5.3.2. Запрещается отправлять файлы, содержащие персональные данные в открытом виде (незашифрованные).

5.3.3. Запрещается массовая рассылка почтовых сообщений (более 10) внешним адресатам без согласования с руководством (спама).

5.3.4. Запрещается использовать не свой обратный адрес при отправке электронной почты.

5.3.5. Запрещается отправлять по электронной почте исполняемые файлы (обычно имеют расширения exe, com, bat). В случае необходимости отправки таких файлов, помещать их в архив.

5.3.6. Присоединяемые файлы рекомендуется упаковывать в архив при помощи программ-архиваторов.

5.3.7. Корпоративные рекомендации использования электронной почты:

– Вы должны оказывать то же уважение, что и при устном общении;

– Вы должны проверять правописание, грамматику и дважды перечитывать свое сообщение перед отправлением;

– Вы не должны участвовать в рассылке посланий, пересылаемых по цепочке (чаще всего это письма религиозно-мистического, развлекательного содержания, спам);

– Вы не должны по собственной инициативе пересылать по произвольным адресам незатребованную информацию;

– Вы не должны рассылать сообщения, которые являются

– Вы не должны рассылать сообщения, которые являются зловредными, раздражающими или содержащими угрозы другим пользователям;

– Вы не должны отправлять никаких сообщений противозаконного или неэтичного содержания;

– Вы должны помнить, что электронное послание является эквивалентом почтовой открытки и не должно использоваться для пересылки конфиденциальной информации без использования средств защиты (шифрование);

– Вы не должны использовать широковещательные возможности электронной почты за исключением выпуска уместных объявлений;

– Вы должны свести к минимуму количество электронных посланий личного характера.

6. Порядок работы с носителями информации

6.1. Под использованием носителей информации в информационных системах Отдела понимается их подключение к инфраструктуре информационных систем с целью обработки, приема/передачи информации между информационными системами и носителями информации.

6.2. Допускается использование только учтенных носителей информации, которые являются собственностью Отдела и подвергаются регулярной ревизии и контролю.

6.3. Учет и выдачу съемных носителей информации осуществляет администратор. Факт выдачи носителя фиксируется в журнале учета съемных носителей информации, форма которого утверждается приказом ректора.

6.4. Возможность подключения носителей информации, а также получение учтенных носителей информации предоставляются Пользователям по инициативе руководителя в случаях:

– необходимости выполнения вновь принятым работником своих должностных обязанностей;

– возникновения у Пользователя производственной необходимости.

6.5. При использовании носителей информации необходимо:

– использовать носители информации исключительно для выполнения своих служебных обязанностей;

– бережно относится к носителям конфиденциальной информации;

– обеспечивать физическую безопасность носителей информации всеми разумными способами;

– извещать руководителя о фактах утраты (кражи) носителей информации.

6.6. При использовании носителей конфиденциальной информации запрещено: – использовать носители конфиденциальной информации в личных целях;

– передавать носители конфиденциальной информации другим лицам

(за исключением администраторов);

– хранить съемные носители с конфиденциальной информацией (персональными данными) на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

– выносить съемные носители с конфиденциальной информацией (персональными данными) из служебных помещений для работы с ними на дому и т. д.

6.7. Любое взаимодействие (обработка, прием/передача информации), инициированное Пользователем между информационной системой и неучтенными (личными) носителями информации, рассматривается как несанкционированное. 6.8. В случае выявления фактов несанкционированного и/или нецелевого использовании носителей информации инициируется служебная проверка, проводимая комиссией, состав которой утверждается руководителем. По факту выясненных обстоятельств составляется акт расследования инцидента и передается руководителю структурного подразделения для принятия мер согласно локальным нормативным актам Отдела и действующему законодательству Российской Федерации.

6.9. При отправке или передаче конфиденциальной информации (персональных данных) адресатам на съемные носители записываются только предназначенные адресатам данные.

6.10. Вынос съемных носителей конфиденциальной информации (персональных данных) для непосредственной передачи адресату осуществляется только с разрешения руководителя.

6.11. Съемные носители конфиденциальной информации (персональных данных), пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссией, состав которой определяется ответственным за организацию обработки персональных данных. По результатам уничтожения носителей составляется акт.

6.12. В случае увольнения работника предоставленные носители конфиденциальной информации изымаются и делаются соответствующие пометки в журнале учета носителей.

7. Права пользователя

7.1. Использовать информационные системы Отдела для выполнения служебных обязанностей.

7.2. Обращаться к ответственному за организацию обработки персональных данных для консультаций по поводу использования программного обеспечения, вопросам обработки персональных данных.

7.3. Направлять предложения по установке новых версий существующего программного обеспечения (с обоснованием необходимости

замены старых версий на новые).

7.4. Направлять предложения по модернизации программного обеспечения.

7.5. Направлять предложения по установке нового (а также дополнительного) программного обеспечения (с указанием цели использования, преимуществ перед существующими аналогами).

7.6. Направлять предложения по модернизации АРМ (замены на новые аналоги), входящих в ИСПДн (с обязательным обоснованием замены и указанием преимуществ перед существующими аналогами).

7.7. Получать консультации и разъяснения по нормативным документам, регламентирующим работу с персональными данными в Отделе.

8. Ответственность

8.1. Пользователь несет персональную ответственность за свои действия или бездействие, которые повлекут за собой разглашение персональных данных, а также за нарушение нормального функционирования информационных систем или ее отдельных компонентов, несанкционированный доступ к информации в соответствие с законодательством Российской Федерации и локальными нормативными актами Отдела.

С инструкцией ознакомлен:

_____ (_____)
_____ (_____)
_____ (_____)
_____ (_____)

Приложение 12

УТВЕРЖДЕНО:
приказом муниципального бюджетного учреждения культуры «Староминский историко-краеведческого музея» муниципального образования Староминский район
от 23 мая 2023 года № 78

Инструкция
по рассмотрению обращений субъектов персональных данных и их законных представителей

1. Общие положения

1.1. Настоящая «Инструкция по рассмотрению обращений субъектов персональных данных и их представителей» (далее — Инструкция) определяет порядок обработки поступающих в муниципальное бюджетное учреждение культуры «Староминский историко-краеведческий музей» муниципального образования Староминский район обращений субъектов персональных данных (далее — Оператор) в соответствии с требованиями Федеральногозакона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), Постановления Правительства от 21 марта 2012 г. №211 «Об утверждении перечнямер, направленных на обеспечение выполнения обязанностей, предусмотренныхФедеральным законом «О персональных данных» и принятыми в соответствии с нимнормативными правовыми актами, операторами, являющимися государственными илимуниципальными органами» и иными нормативными правовыми актами РФ в областизащиты персональных данных.

1.2. С Инструкцией знакомится под подпись ответственный за организацию обработкиперсональных данных.

2. Права субъектов персональных данных

2.1. В соответствии с ч. 7 ст. 14 ФЗ «О персональных данных» субъект персональных данныхимеет право на получение информации в доступной форме, касающейся обработки егоперсональных данных, в том числе содержащей:

— подтверждение факта обработки персональных данных Оператором;
— правовые основания и цели обработки персональных данных;
— способы обработки персональных данных, применяемые Оператором;

— сведения о лицах, которые имеют доступ к персональным данным или которым можетбыть предоставлен доступ на основании договора или федерального закона;
— перечень обрабатываемых персональных данных субъекта и источник их получения;
— сроки обработки персональных данных и сроки их хранения;
— порядок осуществления субъектом персональных данных прав, предусмотренных ФЗ «Оперсональных данных»;
— сведения о наличии трансграничной передачи;
—наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработкуперсональных данных по поручению Оператора, если обработка поручена или будетпоручена такому лицу.

2.2. Право субъекта персональных данных на доступ к его персональным данным можетбыть ограничено в случае, если:
— обработка персональных данных, в том числе полученных в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;
— обработка персональных данных осуществляется органами, осуществившими задержаниесубъекта персональных данных по подозрению в совершении преступления, либопредъявившими субъекту персональных данных обвинение по уголовному делу, либоприменившими к субъекту персональных данных меру пресечения до предъявленияобвинения, за исключением предусмотренных уголовно-процессуальнымзаконодательством РФ случаев, если допускается ознакомление подозреваемого илиобвиняемого с такими персональными данными;
— доступ субъекта персональных данных к его персональным данным нарушает права изаконные интересы третьих лиц;
— в иных случаях, предусмотренных ч. 8 ст. 14 ФЗ «О персональных данных».

2.3. Субъект персональных данных вправе требовать от Оператора уточнения своихперсональных данных, блокирования или их уничтожения в случае, если персональныеданные являются неполными, устаревшими, неточными, незаконно полученными или неявляются необходимыми для заявленной цели обработки.

2.4. Субъект персональных данных вправе принимать предусмотренные законом меры позащите своих прав.

2.5. Если сведения, указанные в пункте 2.1 Инструкции, были предоставлены субъектуперсональных данных, то повторно субъект может обратиться не ранее чем через тридцатьдней после первоначального обращения. Если предоставленные сведения были неполными, то субъект может обратиться повторно до истечения тридцати дней. Обращение должно содержать обоснование направления повторного обращения.

3. Порядок работы с обращениями субъектов персональных данных

3.1. Оператор отвечает на обращения субъектов персональных данных или их законныхпредставителей в сроки установленные ФЗ «О персональных данных» (Приложение).

3.2. При поступлении обращения субъекта или его законного представителя, ответственныйза организацию обработки персональных данных регистрирует обращение в «Журнале учёта обращений субъектов персональных данных и их законных представителей» (Приложение 2).

3.3. При поступлении обращения субъекта или его законного представителя, Оператор предоставляет информацию о персональных данных субъекта в течение тридцати дней (Приложение 3).

3.4. В случае отзыва субъектом персональных данных согласия на их обработку, она можетбыть продолжена при наличии оснований, указанных в п. 2—11 ч. 1 ст. 6, ч. 2 ст. 10 и ч. 2 ст.11 ФЗ «О персональных данных».

3.5. В случае отказа в предоставлении информации субъекту персональных данных или егозаконному представителю, Оператор даёт в письменной форме мотивированный ответ втечение тридцати дней со дня обращения либо с даты получения обращения.

3.6. При предоставлении субъектом или его законным представителем сведений,подтверждающих, что персональные данные субъекта являются неполными, устаревшими,недостоверными, незаконно полученными или не являются необходимыми для заявленнойцели обработки, Оператор вносит в них необходимые изменения, уничтожает илиблокирует. О внесенных изменениях и предпринятых мерах Оператор уведомляет субъектаперсональных данных или его законного представителя и третьих лиц, которымперсональные данные субъекта были переданы (Приложение 4).

3.7. При отсутствии сведений, подтверждающих, что персональные данные субъекта являются неполными, устаревшими, недостоверными, незаконно полученными или неявляются необходимыми для заявленной цели обработки, Оператор отказывается вноситьизменения и даёт ответ субъекту персональных данных (Приложение 5).

3.8. Оператор сообщает в уполномоченный орган по защите прав субъектов персональныхданных по его запросу информацию, необходимую для осуществления деятельностиуказанного органа, в течение тридцати дней с даты получения такого запроса (Приложение 6).

4. Ответственность

4.1. Ответственный за организацию обработки персональных данных несёт ответственностьв соответствии с действующим законодательством за организацию приёма и обработкиобращений субъектов персональных данных и их законных представителей.

Приложение

К Инструкции по рассмотрению обращений субъектов персональных данных и их законных представителей

**Сводная таблица действий Оператора в ответ на обращения субъектов персональных данных,
их представителей и запросы Уполномоченного органа по защите прав субъектов
персональных данных**

Обращение, запрос	Действия	Срок
Неправомерный доступ третьих лиц к ПД сотрудников	Уведомить Роскомнадзор	в течение 24 часов
по факту доступа третьих лиц к ПД сотрудников	Отчитаться в Роскомнадзор об итогах расследования	в течение 72 часов
о начале обработки ПД сотрудников	Уведомить Роскомнадзор	в течение 10 рабочих дней
об обработке ПД в случаях, если ПД: включены в государственные информационные системы ПД по защите государства и общественного порядка; – когда оператор обрабатывает ПД исключительно без использования средств автоматизации.	Не уведомлять Роскомнадзор	
на запрос Роскомнадзора о работе с ПД	Предоставить ответ	в течение 10 рабочих дней
если сведения из уведомления о начале обработки ПД изменились	Уведомить Роскомнадзор,	до 15 числа месяца, следующего за месяцем, когда произошли изменения
Взаимодействие с сотрудником или иным субъектом персональных данных		
Наличие персональных данных	Подтверждение обработки персональных данных	в течение 10 рабочих дней, с продлением на 5 рабочих дней**(Направление мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации);
	Отказ от подтверждения обработки персональных данных	

Уточнение ПД	Уведомление о внесенных изменениях	7 рабочих дней со дня предоставления уточняющих сведений
Ознакомление с персональными данными Предоставление информации по ПД: 1.Подтверждение обработки персональных данных, правовые основания и цели такой обработки 2. Способы обработки ПД; 3.Сведения о лицах, которые имеют доступ к ПД; 4.Перечень обрабатываемых персональных данных и источник их Получения; 5.Сроки обработки ПД, в том числе сроки их хранения; 6.Информация об осуществленной или о предполагаемой трансграничной передаче	Предоставить информацию по персональным данным	В течение 10 рабочих дней, с продлением на 5 рабочих дней* *(Направление мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации); При повторном запросе не ранее чем через тридцать дней после первоначального обращения
разъяснение субъекту ПД о автоматизированной обработки его персональных данных.	рассмотреть возражения	30 дней
Содержание уведомления о намерении получить персональные данные у третьих лиц	Предоставить ответ	в дополнение к прежнему: – категории ПД, которые будете запрашивать
Предоставлять биометрические данные сотрудником работодателю		сотрудник вправе отказаться
Хранить биометрические данные несовершеннолетних**		**запрещено**
Отзыв согласия на обработку персональных данных	Прекращение обработки и уничтожение персональных данных	Уведомление о прекращении обработки и уничтожении персональных данных 30 дней
	Отказ от прекращения обработки и уничтожения персональных данных	Уведомление об отказе прекращения обработки и уничтожения персональных данных 30 дней
Неправомерность действий с персональными данными субъекта	Уведомление об устранении нарушений	3 рабочих дня
	Уничтожение персональных данных в случае	10 рабочих дня

	невозможности обеспечения правомерности обработки	
Достижение цели обработки персональных данных субъекта	Прекращение обработки персональных данных	Уведомление об уничтожении персональных данных 30 дней
	Уничтожение персональных данных	
Прекращение обработки ПД по требованию работника	Прекращение обработки персональных данных	в течение 10 рабочих дней, с продлением на 5 рабочих дней* *(Направление мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации)
В случае отсутствия возможности уничтожения персональных данных в течение срока		блокирование и уничтожение персональных данных в срок не более чем шесть месяцев
Уничтожение персональных данных		Уведомление об уничтожении