КонсультантПлюс

Распоряжение Мингосуправления МО от 01.03.2023 N 11-27/РВ
"Об организации работ по защите персональных данных и иной информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, в Министерстве государственного управления, информационных технологий и связи Московской области"
(вместе с "Перечнем сведений, отнесенных к информации ограниченного доступа, и персональных данных, обрабатываемых в Министерстве государственного управления, информационных технологий и связи Московской области", "Положением по обработке и защите информации ограниченного доступа, не составляющей государственную тайну, включая персональные данные", "Положением о порядке учета, хранения и обращения со съемными носителями персональных данных и иной информации ограниченного доступа", "Правилами рассмотрения запросов субъектов персональных данных или их представителей", "Правилами осуществления внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации", "Правилами работы с обезличенными данными", "Перечнем должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных", "Перечнем должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным", "Инструкцией должностного лица, ответственного за организацию обработки персональных данных в Министерстве государственного управления, информационных технологий и связи Московской области", "Порядком доступа сотрудников в помещения, в которых ведется обработка персональных данных и иной информации ограниченного доступа", "Инструкцией пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций")

МИНИСТЕРСТВО ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ МОСКОВСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ
от 1 марта 2023 г. N 11-27/РВ

ОБ ОРГАНИЗАЦИИ РАБОТ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, НЕ СОДЕРЖАЩЕЙ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ, В МИНИСТЕРСТВЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ МОСКОВСКОЙ ОБЛАСТИ

В целях выполнения требований федеральных законов от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 21 марта 2012 г. N 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", нормативных правовых актов Российской Федерации, руководящих и методических документов ФСБ России, ФСТЭК России и Роскомнадзора, постановления Правительства Московской области от 29 июля 2020 г. N 469/21 "Об утверждении Порядка обработки информации ограниченного доступа в исполнительных органах государственной власти Московской области, государственных органах Московской области и государственных учреждениях Московской области и признании утратившими силу некоторых постановлений Правительства Московской области" в соответствии с Положением о Министерстве государственного управления, информационных технологий и связи Московской области, утвержденным постановлением Правительства Московской области от 13 июня 2012 г. N 820/19:

1. Назначить ответственным должностным лицом за организацию обработки персональных данных в Министерстве государственного управления, информационных технологий и связи Московской области (далее - Министерство) И.А. Гиренко - первого заместителя министра государственного управления, информационных технологий и связи Московской области.

2. Возложить полномочия по обеспечению информационной безопасности в Министерстве, в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты, на С.А. Коношенко - заместителя министра государственного управления, информационных технологий и связи Московской области.

3. Назначить ответственным должностным лицом за выполнение работ по защите информации и контроль соблюдения организационно-технических и режимных мер по защите информации в структурных подразделениях Министерства С.А. Науменко - заместителя начальника Управления информационной безопасности.

4. Назначить ответственным должностным лицом за рассмотрение запросов и обращений субъектов персональных данных (представителей субъектов персональных данных), поступивших в Министерство, А.В. Мозгового - заместителя начальника управления - заведующего отделом обеспечения информационной безопасности региональных информационных систем и ресурсов

Управления информационной безопасности.

5. Утвердить:

перечень сведений, отнесенных к информации ограниченного доступа, и персональных данных, обрабатываемых в Министерстве государственного управления, информационных технологий и связи Московской области (приложение N 1);

Положение по обработке и защите информации ограниченного доступа, не составляющей государственную тайну, включая персональные данные (приложение N 2);

Положение о порядке учета, хранения и обращения со съемными носителями персональных данных и иной информации ограниченного доступа (приложение N 3);

Правила рассмотрения запросов субъектов персональных данных или их представителей (приложение N 4);

Правила осуществления внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации (приложение N 5);

Правила работы с обезличенными данными (приложение N 6);

перечень должностей, при замещении которых устанавливается ответственность за проведение мероприятий по обезличиванию обрабатываемых персональных данных (приложение N 7);

перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо доступа к персональным данным (приложение N 8);

инструкцию должностного лица, ответственного за организацию обработки персональных данных в Министерстве государственного управления, информационных технологий и связи Московской области (приложение N 9);

типовое обязательство гражданского служащего (сотрудника), непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных (служебных) обязанностей (приложение N 10);

типовые формы согласий на обработку персональных данных (приложение N 11);

типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение N 12);

Порядок доступа сотрудников в помещения, где проводится обработка персональных данных и иной информации ограниченного доступа (приложение N 13);

типовую форму акта об уничтожении персональных данных (информации ограниченного доступа) (приложение N 14);

инструкцию пользователя по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций (приложение N 15);

типовую форму журнала учета событий информационной безопасности (приложение N 16);

типовую форму обязательства о неразглашении информации ограниченного доступа (приложение N 17);

типовую форму журнала учета машинных носителей персональных данных и иной информации ограниченного доступа (приложение N 18);

типовую форму акта расследования инцидента (приложение N 19).

6. Признать утратившими силу пункты 1 - 5 и 7 распоряжения Министерства государственного управления, информационных технологий и связи Московской области от 08.04.2021 N 11-31/РВ "Об организации работ по защите информации ограниченного доступа, не составляющей государственную тайну, включая персональные данные, в информационных системах Министерства государственного управления, информационных технологий и связи Московской области".

7. Управлению бухгалтерского учета, правовой и кадровой работы в пятидневный срок обеспечить размещение настоящего распоряжения на официальном сайте Министерства в сети Интернет.

8. Контроль за исполнением настоящего распоряжения оставляю за собой.

Министр государственного управления,
информационных технологий и связи
Московской области
Н.В. Куртяник

Приложение N 1
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПЕРЕЧЕНЬ
СВЕДЕНИЙ, ОТНЕСЕННЫХ К ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, И ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В МИНИСТЕРСТВЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ МОСКОВСКОЙ ОБЛАСТИ

N п/п	Содержание сведений	Основание для включения в перечень
1.	Сведения о частной жизни, личной и семейной тайне, переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях	Конституция Российской Федерации (статьи 23, 24)
2.	Сведения, содержащие персональные данные (за исключением персональных данных общедоступных категорий)	Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"
3.	Сведения, содержащие служебную информацию, ставшую известной государственному гражданскому служащему в связи с исполнением должностных обязанностей	Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации" (статья 17)
4.	Сведения об абонентах и оказываемых им услугах связи	Федеральный закон от 07.07.2003 N 126-ФЗ "О связи" (статья 53)
5.	Сведения, ставшие известными работнику органа записи актов гражданского состояния или работнику многофункционального центра предоставления государственных и муниципальных услуг в связи с государственной регистрацией акта гражданского состояния	Федеральный закон от 15.11.1997 N 143-ФЗ "Об актах гражданского состояния" (статья 6)
6.	Сведения о доходах, об имуществе и обязательствах имущественного характера	Федеральный закон от 27.07.2004 N 79-ФЗ "О государственной гражданской службе Российской Федерации" (статья 20)
7.	Сведения о населении, содержащиеся в переписных листах	Федеральный закон от 25.01.2002 N 8-ФЗ "О Всероссийской переписи населения" (статья 8)
8.	Сведения, содержащиеся в индивидуальных лицевых счетах	Федеральный закон от 01.04.1996 N 27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования" (статья 6)
9.	Сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их	Гражданский кодекс Российской Федерации (статья 946)

	здоровья, а также об имущественном положении этих лиц	
10.	Сведения, содержащие информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, в отношении которых их обладателем установлен режим коммерческой тайны (за исключением информации, в отношении которой имеется согласие другой стороны на передачу информации третьим лицам)	Гражданский кодекс Российской Федерации (статья 727)
11.	Сведения о частной жизни лица, подавшего жалобу, и других лиц, ставшие известными Уполномоченному по правам человека в субъекте Российской Федерации в процессе рассмотрения жалобы, без их письменного согласия	Федеральный закон от 06.10.1999 N 184-ФЗ "Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации" (статья 16.1); Федеральный закон от 18.03.2020 N 48-ФЗ "Об уполномоченных по правам человека в субъектах Российской Федерации" (статья 10)
12.	Сведения о местах дислокации или о передислокации органов управления войсками национальной гвардии, объединений, соединений, воинских частей войск национальной гвардии, а также обеспечивается конфиденциальность сведений о военнослужащих (сотрудниках) войск национальной гвардии и членах их семей	Федеральный закон от 03.07.2016 N 226-ФЗ "О войсках национальной гвардии Российской Федерации" (статья 23)
13.	Сведения, содержащие информацию, полученную в ходе действий должностных лиц органа государственного контроля при проведении проверок российских участников внешнеэкономической деятельности	Федеральный закон от 18.07.1999 N 183-ФЗ "Об экспортном контроле" (статья 17)
14.	Сведения, касающихся предмета договора на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода его	Гражданский кодекс Российской Федерации (статья 771)

	исполнения и полученных результатов (в объеме, определенном договором)	
15.	Сведения, полученные пользователем по договору коммерческой концессии, содержащие секреты производства (ноу-хау) правообладателя и другую полученную от него конфиденциальную коммерческую информацию	Гражданский кодекс Российской Федерации (статья 1032)
16.	Сведения о данных предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения	Уголовный кодекс Российской Федерации (статья 310); Уголовно-процессуальный кодекс Российской Федерации (статья 161)
17.	Сведения, содержащие: суждения, имевшие место во время совещания суда присяжных заседателей в совещательной комнате; суждения, имевшие место при обсуждении и постановлении приговора	Уголовно-процессуальный кодекс Российской Федерации (статьи 298, 341)
18.	Сведения о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судебного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса, а равно в отношении их близких	Уголовный кодекс Российской Федерации (статья 311)
19.	Сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа, а также его близких	Уголовный кодекс Российской Федерации (статья 320)
20.	Конфиденциальные сведения о музейных предметах, включенных в состав негосударственной части Музейного фонда Российской Федерации	Федеральный закон от 26.05.1996 N 54-ФЗ "О Музейном фонде Российской Федерации и музеях в Российской Федерации" (статья 38)
21.	Первичные статистические данные, содержащиеся в формах федерального статистического наблюдения	Федеральный закон от 29.11.2007 N 282-ФЗ "Об официальном статистическом учете и системе государственной статистики в Российской Федерации" (статья 9)

22.	Сведения, содержащиеся в анкете ребенка, гражданина, желающего принять ребенка на воспитание в свою семью, гражданина, лишенного родительских прав или ограниченного в родительских правах, гражданина, отстраненного от обязанностей опекуна (попечителя) за ненадлежащее выполнение возложенных на него законом обязанностей, бывшего усыновителя, если усыновление отменено судом по его вине	Федеральный закон от 16.04.2001 N 44-ФЗ "О государственном банке данных о детях, оставшихся без попечения родителей" (статья 8)
23.	Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны	Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне" (статья 3)
24.	Сведения о специальных средствах, технических приемах, тактике осуществления мероприятий по борьбе с терроризмом, а также о составе их участников	Федеральный закон от 06.03.2006 N 35-ФЗ "О противодействии терроризму" (статья 2)
25.	Сведения, указанные в документах, поступивших в Министерство из иных организаций, и имеющих ограничительные пометки	Ограничительные пометки поступивших в Министерство документов

Приложение N 2
к распоряжению Министерства
государственного управления,

информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПОЛОЖЕНИЕ ПО ОБРАБОТКЕ И ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ВКЛЮЧАЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

1. Общие положения

1.1. Настоящее Положение по обработке и защите информации ограниченного доступа, не составляющей государственную тайну, включая персональные данные (далее - Положение, ИОД, соответственно) разработано на основании Федеральных законов от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлений Правительства Российской Федерации от 21 марта 2012 г. N 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", от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", приказа ФСТЭК России от 18 февраля 2013 г. N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", приказа Роскомнадзора от 28 октября 2022 г. N 179 "Об утверждении Требований к подтверждению уничтожения персональных данных", постановления Правительства Московской области от 29 июля 2020 N 469/21 "Об утверждении Порядка обработки информации ограниченного доступа в исполнительных органах государственной власти Московской области, государственных органах Московской области и государственных учреждениях Московской области и признании утратившими силу некоторых постановлений Правительства Московской области", а также нормативных правовых актов и методических документов по вопросам безопасности персональных данных (далее - ПДн) при их обработке в информационных системах (далее - ИС), в том числе информационных системах персональных данных (далее - ИСПДн).

1.2. В Положении используются следующие термины:

информация - сведения (сообщения, данные) независимо от формы их представления;

информация ограниченного доступа (ИОД) - информация, доступ к которой ограничен законодательством Российской Федерации;

персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационная система персональных данных (ИСПДн) - совокупность содержащихся в

базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств;

оператор ИС - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

оператор ПДн - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;

обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники;

распространение информации (ПДн) - действия, направленные на раскрытие информации (ПДн) неопределенному кругу лиц;

предоставление информации (ПДн) - действия, направленные на раскрытие информации (ПДн) определенному лицу или определенному кругу лиц;

блокирование информации (ПДн) - временное прекращение обработки информации (ПДн), за исключением случаев, если обработка необходима для уточнения ПДн;

уничтожение информации (ПДн) - действия, в результате которых становится невозможным восстановить содержание информации (ПДн) в ИС и (или) в результате которых уничтожаются материальные носители информации (ПДн);

обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн;

трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Настоящее Положение определяет порядок и условия обработки ИОД в Министерстве государственного управления, информационных технологий и связи Московской области (далее - Министерство), включая порядок передачи ИОД третьим лицам, особенности автоматизированной и неавтоматизированной их обработки ИОД, порядок доступа к ИОД, систему защиты ИОД, порядок организации внутреннего контроля и ответственность за нарушения при обработке ИОД.

1.4. Требования к порядку обработки ИОД, указанные в настоящем Положении,

предъявляются в том числе и к порядку обработки ПДн. При этом в отношении ПДн могут предъявляться дополнительные требования, указанные в отдельных пунктах Положения.

1.5. Действие настоящего Положения распространяется на все процессы обработки ИОД в Министерстве, включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение (в том числе передачу), блокирование, уничтожение ИОД, а также обезличивание ПДн, осуществляемые с использованием средств автоматизации и без их использования.

1.6. Настоящее Положение вступает в силу с момента его утверждения министром государственного управления, информационных систем и связи Московской области (далее - министр) и действует бессрочно до замены его новым Положением.

1.7. Все изменения в Положение вносятся распоряжением Министерства либо приказом министра.

1.8. Все сотрудники Министерства, участвующие в процессах обработки ИОД в Министерстве, должны быть ознакомлены с настоящим Положением в установленном в Министерстве порядке.

2. Цели и задачи обработки ИОД

2.1. Обработка ИОД осуществляется на законной и справедливой основе и ограничивается достижением конкретных, заранее определенных и законных целей.

2.2. Обработка ИОД в Министерстве осуществляется в целях реализации возложенных на Министерство задач, исполнения государственных функций и полномочий Министерства.

2.3. Особенности обработки ИОД, содержащей ПДн.

2.3.1. Не допускается обработка ПДн, несовместимая с заявленными целями сбора ПДн. Обработке подлежат только ПДн, которые отвечают целям их обработки.

2.3.2. Не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой.

2.3.3. Содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки.

2.3.4. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

2.3.5. Основными целями обработки ПДн является:

обеспечение прав граждан, организаций, органов государственной власти и органов местного самоуправления на поиск, получение, передачу, производство и распространение информации;

внедрение информационно-телекоммуникационных технологий в процедуры предоставления государственных услуг населению и организациям;

реализация возложенных на Министерство задач, исполнение государственных функций и полномочий Министерства;

контроль за предоставлением государственных и муниципальных услуг на территории Московской области;

заключение трудовых отношений с физическими лицами; выполнение договорных обязательств Министерства; соблюдение действующего законодательства Российской Федерации.

2.3.6. ИСПДн обеспечивают решение следующих задач:

упрощение процедуры обработки ПДн, сокращение времени на их обработку;

контроль использования ПДн;

защита ПДн, в том числе воспрепятствование неправомерному доступу к ПДн;

объединение в едином хранилище данных, предоставленных субъектами, с учетом требований законодательства Российской Федерации;

обмен ПДн с использованием информационных систем связи и передачи информации.

3. Информация ограниченного доступа, обрабатываемая в Министерстве

3.1. Перечень ИОД, обрабатываемой в Министерстве, указан в приложении 1 к настоящему распоряжению. Изменения в перечень ИОД, обрабатываемой в Министерстве, вносятся распоряжениями Министерства либо приказами министра.

3.2. ПДн, обрабатываемые в Министерстве.

3.2.1. В Министерстве обрабатываются ПДн сотрудников Министерства и лиц, не являющихся сотрудниками Министерства.

3.2.2. ПДн субъектов ПДн могут включать:

специальные категории ПДн;

общедоступные ПДн;

иные категории ПДн.

Обработка биометрических ПДн в Министерстве не осуществляется.

3.2.3. Полные списки обрабатываемых ПДн формируются в перечнях ПДн, подлежащих защите (либо иных организационно-распорядительных документах), в ИСПДн Министерства.

4. Доступ к ИОД

4.1. Сотрудники Министерства, которые в силу выполняемых служебных обязанностей постоянно работают с ИОД, получают допуск к необходимой информации на срок выполнения ими соответствующих должностных обязанностей в соответствии с утвержденными министром перечнями лиц (должностей), допущенных к работе с ИОД.

4.2. Списки лиц (должностей), имеющих доступ к ИОД, должны поддерживаться в актуальном состоянии.

4.3. Министерством установлен разрешительный порядок доступа к ИОД. Сотрудникам предоставляется доступ к работе с ИОД исключительно в пределах и объеме, необходимых для выполнения ими своих должностных обязанностей.

4.4. В целях реализации возложенных на Министерство задач, исполнения государственных функций и полномочий Министерства отдельные функции обработки ИОД, могут осуществляться сотрудниками подведомственных Министерству учреждений, с учетом требований законодательства Российской Федерации. В данном случае права и обязанности указанных сотрудников, связанные с обработкой ИОД и описанные в настоящем Положении, соответствуют правам и обязанностям сотрудников Министерства.

4.5. Временный или разовый допуск к работе с ИОД в связи со служебной необходимостью может быть получен сотрудником Министерства по согласованию с министром и руководителями структурных подразделений Министерства без внесения изменений списка лиц (должностей), допущенных к работе с ИОД.

4.6. В случае если сотруднику сторонней организации требуется доступ к ИОД Министерства, необходимо, чтобы в договоре со сторонней организацией (ином документе о взаимодействии между Министерством и сторонней организацией) были прописаны условия конфиденциальности ИОД и обязанность сторонней организации и ее сотрудников по соблюдению требований законодательства Российской Федерации в области обработки и защиты ИОД, а также, в случае передачи ПДн - обработки и защиты ПДн.

4.7. Доступ сотрудника Министерства к ИОД прекращается с даты завершения трудовых отношений либо с даты изменения должностных обязанностей сотрудника и (или) исключения его из списков лиц, имеющих право доступа к ИОД. В случае увольнения все находившиеся в распоряжении сотрудника в соответствии с его должностными обязанностями носители, содержащие ИОД, передаются руководителям структурных подразделений.

4.8. Доступ к обрабатываемым в Министерстве ПДн со стороны третьих лиц (не являющихся сотрудниками Министерства и подведомственных Министерству учреждений) без согласия субъекта ПДн запрещен, если иное не определено законодательством Российской Федерации либо если передача ПДн третьим лицам необходима для достижения цели, на обработку ПДн для реализации которой получено согласие субъекта ПДн.

5. Основные требования по защите ИОД

5.1. При обработке ИОД в информационных системах Министерства обеспечивается:

определением угроз безопасности ИОД при ее обработке в информационных системах;

проведением мероприятий, направленных на предотвращение несанкционированного доступа к ИОД и (или) передачи ее лицам, не имеющим права доступа к такой информации, в том числе применением организационных и технических мер по обеспечению безопасности ИОД;

применением средств защиты информации, имеющих сертификаты соответствия требованиям ФСТЭК России (для средств криптографической защиты информации - ФСБ России);

своевременное обнаружение фактов несанкционированного доступа к ИОД;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущением воздействия на технические средства обработки ИОД, в результате которого может быть нарушено их функционирование;

возможностью незамедлительного восстановления ИОД, модифицированной или уничтоженной вследствие несанкционированного доступа;

постоянным контролем обеспечения требований к защищенности ИОД и требуемого уровня защищенности ПДн (при наличии);

оценкой эффективности (аттестацией по требованиям информационной безопасности) принимаемых мер по обеспечению безопасности ИОД до ввода в эксплуатацию ИС и начала обработки ИОД в ней;

обнаружением фактов несанкционированного доступа к ИОД и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы и по реагированию на компьютерные инциденты в них;

восстановлением ИОД, модифицированной или уничтоженной вследствие несанкционированного доступа;

нахождением на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение ПДн граждан Российской Федерации.

5.2. Министерство принимает необходимые правовые, организационные и технические меры для обеспечения безопасности ИОД.

5.3. На основании нормативных правовых актов и методических документов ФСТЭК России и ФСБ России для установления требований по обеспечению безопасности и внедрения системы обеспечения безопасности ИОД в Министерстве разрабатывается комплект организационно-распорядительной документации (для каждой ИС, предназначенной для обработки ИОД) и модель угроз безопасности информации при ее обработке в ИС (для каждой ИСПДн и (или) государственной ИС (далее - ГИС) Министерства). Модели угроз безопасности информации для

ИС Министерства, имеющих статус ГИС, подлежат согласованию с ФСТЭК России и ФСБ России в пределах их полномочий.

В случае необходимости применения в ИС средств криптографической защиты информации (далее - СКЗИ) при разработке модели угроз также разрабатывается модель нарушителя информационной безопасности, в которой определяются требования к классам применяемых СКЗИ.

5.4. В соответствии с приказом ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" членами комиссии по обследованию режимных помещений, категорированию и классификации объектов информатизации Министерства, назначенными приказом министра, проводится классификация ИС.

В соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" членами комиссии по обследованию режимных помещений, категорированию и классификации объектов информатизации Министерства, назначенными приказом министра, проводится классификация (определение требуемого уровня защищенности обрабатываемых в ИСПДн ПДн) ИСПДн.

5.5. В соответствии с приказами ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" и от 18 февраля 2013 г. N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (для ИСПДн) в Министерстве разрабатывается и внедряется комплекс мер по защите и обеспечению безопасности ИОД.

5.6. Эффективность принятых мер по защите и обеспечению безопасности ИОД в ГИС оценивается в рамках аттестации ГИС на соответствие требованиям о защите информации ограниченного доступа, проводимой в соответствии с требованиями, утвержденными приказом ФСТЭК России от 29 апреля 2021 г. N 77.

Эффективность принятых мер по защите и обеспечению безопасности ИОД в ИС, не являющихся ГИС, рекомендуется оценивать в рамках аттестации ГИС на соответствие требованиям о защите информации ограниченного доступа, проводимой в соответствии с требованиями, утвержденными приказом ФСТЭК России от 29 апреля 2021 г. N 77, при этом допускаются другие предусмотренные законодательством Российской Федерации способы оценки эффективности.

5.7. ИОД допускается обрабатывать только в ИС, имеющих актуальные (действующие) документы, оформленные по результатам проведения мероприятий по оценке эффективности принятых мер по защите и обеспечению безопасности ИОД в ИС (аттестации ИС на соответствие требованиям информационной безопасности). При этом в документах должна быть указана возможность обработки ИОД (при необходимости - соответствующего типа ИОД) в ИС.

5.8. Все лица, допущенные к работе с ИОД, а также связанные с эксплуатацией и

техническим сопровождением ИС, должны быть ознакомлены с требованиями настоящего Положения, а также должны соблюдать требования законодательства Российской Федерации в области защиты информации и обработки ПДн (в случае обработки ПДн).

5.9. В Министерстве организуется процесс обучения использованию средств защиты ИОД, обязательный для лиц, ответственных за эксплуатацию средств защиты информации ИС, и рекомендательный для лиц, имеющих постоянный доступ к ИОД, и лиц, эксплуатирующих технические и программные средства ИС и средства защиты ИС.

5.10. Сотрудники Министерства обязаны незамедлительно сообщать руководителям структурных подразделений об утрате или недостаче носителей ИОД, о причинах и условиях возможной утечки ИОД, о попытках посторонних лиц получить от сотрудника ИОД, обрабатываемую Министерством, а также о других случаях, создающих предпосылки для нарушения безопасности обрабатываемой в Министерстве ИОД.

5.11. Отдельные функции по защите обрабатываемой в Министерстве ИОД могут в установленном порядке быть делегированы подведомственным Министерству учреждениям с учетом требований законодательства Российской Федерации.

6. Порядок обработки и защиты ИОД

6.1. Обязательным требованием для всех лиц, которым стала известна ИОД, обрабатываемая Министерством, является обеспечение ее конфиденциальности.

При необходимости при обработке ИОД также предъявляются требования по обеспечению ее целостности и доступности.

6.2. ИОД на бумажных носителях, обрабатываемые в Министерстве, хранятся в отделах (у сотрудников), имеющих допуск к обработке соответствующей информации. Носители ИОД не должны оставаться без присмотра. При покидании рабочего места сотрудники, осуществляющие обработку ИОД, должны убирать носители в сейф, запираемый шкаф или иным образом ограничивать несанкционированный доступ к носителям. При утере или порче ИОД и (или) носителей ИОД осуществляется их восстановление (по возможности).

6.3. Порядок обращения с документами, изданиями (книгами, журналами, брошюрами, почтовыми отправлениями) и другими материальными и машинными носителями информации, содержащими ИОД, определяется Правилами делопроизводства в исполнительных органах государственной власти Московской области, государственных органах Московской области, утвержденных постановлением Губернатора Московской области, а также Положением о порядке учета, хранения и обращения со съемными носителями персональных данных и иной информации ограниченного доступа (приложение N 3 к настоящему распоряжению).

6.4. При работе с программными средствами ИС Министерства, реализующих функции просмотра и редактирования ИОД, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

6.5. При получении ИОД сотрудником Министерства, который в соответствии с должностными обязанностями получает ИОД от клиента, сотрудника, иного лица, в обязательном

порядке проводится проверка достоверности ИОД. Ввод ИОД, полученной Министерством, в ИС, осуществляется сотрудниками, имеющими доступ к соответствующей информации.

При этом ввод и обработка ИОД допускается только в ИС, предназначенных для обработки такой информации. Такая возможность должна быть указана в документах, оформляемых по результатам проведения мероприятий по оценке эффективности принятых мер по защите и обеспечению безопасности ИОД в ИС (аттестации ИС по требованиям информационной безопасности).

6.6. Сотрудники, осуществляющие ввод ИОД в ИС, несут ответственность за достоверность и полноту введенной информации, а также за соблюдение требований информационной безопасности при вводе и обработке ими ИОД в ИС (в том числе - в части вопросов соответствия ИС либо ее компонента требованиям информационной безопасности, предъявляемым для возможности обработки ИОД в ИС).

6.7. Обработка ПДн на бумажных носителях, без использования средств автоматизации (в случаях, если при обработке ПДн не используется ПЭВМ) осуществляется в соответствии с требованиями, утвержденными постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687.

6.7.1. При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

6.7.2. При неавтоматизированной обработке ПДн на бумажных носителях не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых несовместимы между собой. При этом ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

6.8. Порядок уничтожения, блокирования и уточнения ИОД.

6.8.1. Уничтожение ИОД, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этой информации с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

6.8.2. Уточнение ИОД при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, если это не допускается техническими особенностями материального носителя - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненной информацией.

6.8.3. По результатам уничтожения ПДн оформляется подтверждающий документ - акт об уничтожении ИОД в соответствии с приложением N 14 к настоящему распоряжению.

6.8.4. В случае если подлежащая удалению ИОД содержит ПДн, обработка которых осуществляется с использованием средств автоматизации, кроме акта об уничтожении ИОД производится выгрузка из журнала регистрации событий в ИС. Выгрузка из журнала регистрации событий должна содержать:

фамилию, имя, отчество (при наличии) субъекта (субъектов) ПДн или иную информацию, относящуюся к субъекту ПДн, чьи ПДн были уничтожены;

перечень категорий уничтоженных ПДн субъекта ПДн;

наименование ИСПДн, из которой были уничтожены ПДн;

причину уничтожения ПДн;

дату уничтожения ПДн.

Если выгрузка из журнала не позволяет указать отдельные из перечисленных выше сведений, недостающие сведения вносятся в акт об уничтожении ПДн.

6.8.5. Акт уничтожения ИОД подписывается комиссией в составе:

глава комиссии - должностное лицо, ответственное за обеспечение информационной безопасности в Министерстве либо должностное лицо, ответственное за организацию обработки ПДн в Министерстве (только в случае удаления ПДн);

члены комиссии - должностные лица, ответственные за функционирование ИС, из которых осуществляется удаление ИОД, должностные лица, обеспечившие уничтожение ИОД из ИС, а также должностное лицо, ответственное за рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей (только в случае удаления ПДн).

Акт об уничтожении ИОД подписывается членами комиссии, собственноручно либо посредством квалифицированной электронной подписи в государственной информационной системе "Межведомственная система электронного документооборота".

Акт об уничтожении ИОД в электронной форме, подписанный посредством квалифицированной электронной подписи в государственной информационной системе "Межведомственная система электронного документооборота", признается электронным документом, равнозначным акту об уничтожении ИОД на бумажном носителе, подписанному собственноручной подписью членов комиссии.

6.8.6. Акт об уничтожении ИОД, а также (при наличии) выгрузка из журнала регистрации событий в ИСПДн подлежат хранению в течение 3 лет с момента уничтожения ИОД.

6.9. Уничтожение носителей, содержащих ИОД.

6.9.1. ИОД на бумажных носителях уничтожается путем использования шредеров (уничтожителей документов), установленных в помещениях Министерства.

6.9.2. ИОД, размещенная на флэш-карте, CD-диске, ином носителе информации, уничтожается путем удаления содержимого носителя (форматирования носителя) или путем нарушения работоспособности флэш-карты или CD-диска.

6.9.3. По результатам уничтожении носителя информации составляется акт об уничтожении ИОД (приложение N 14 к настоящему распоряжению).

6.10. По окончании рабочего дня сотрудники Министерства закрывают в служебных помещениях, в которых могут храниться носители ИОД, окна, запирают данные помещения и включают сигнализацию (при наличии).

6.11. Сетевое оборудование, серверы, предназначенные для обработки ИОД, следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

6.12. Уборка помещений и обслуживание технических средств ИС должны осуществляться под контролем лиц, ответственных за данные помещения и (или) технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ИОД, носителям информации, программным и техническим средствам обработки, передачи и защиты информации в ИС.

6.13. В целях изучения и оценки фактического состояния защищенности ИОД, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения, в Министерстве осуществляется внутренний контроль процесса обработки ИОД.

Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности ИОД направлены на решение следующих задач:

обеспечение соблюдения сотрудниками Министерства требований настоящего Положения и нормативных правовых актов, регулирующих процессы обработки и защиты ИОД, обработки и защиты ПДн;

оценка компетентности персонала, задействованного в обработке ИОД;

обеспечение работоспособности и эффективности технических средств ИС и средств защиты ИОД, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам обеспечения безопасности ИОД;

выявление нарушений установленного порядка обработки ИОД и своевременное предотвращение негативных последствий таких нарушений;

принятие корректирующих мер, направленных на устранение выявленных нарушений в процессе обработки ИОД и в работе технических средств ИС;

разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ИОД по результатам контрольных мероприятий;

осуществление внутреннего контроля исполнения рекомендаций и указаний по устранению нарушений.

Результаты контрольных мероприятий оформляются актами и являются основанием для разработки рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ИОД, по модернизации технических средств ИС и средств защиты ИОД, по обучению и повышению компетентности персонала, задействованного в обработке ИОД.

6.14. В случае нарушения установленного порядка обработки ИОД сотрудники Министерства

несут ответственность в соответствии с разделом 9 настоящего Положения.

7. Передача (предоставление) ИОД

7.1. Предоставление ИОД или доступа к ним третьей стороне должны выполняться на основании:

законодательства Российской Федерации;

договора либо иного основания, существенным условием которого является обеспечение третьей стороной конфиденциальности ИОД и безопасности ИОД при ее обработке;

для ПДн - согласия субъекта ПДн на передачу его ПДн третьей стороне, за исключением случаев, когда такая передача необходима для достижения целей, на обработку ПДн в которых субъект ПДн ранее дал согласие, либо в случаях, когда в соответствии с законодательством Российской Федерации согласие субъекта ПДн на обработку его ПДн не требуется.

8. Особенности обработки ИОД, содержащей ПДн, в Министерстве

8.1. Согласие на обработку ПДн.

8.1.1. Субъект ПДн принимает решение о предоставлении своих ПДн и дает согласие на их обработку свободно, по своей воле и в своих интересах. Согласие на обработку ПДн должно быть конкретным, предметным, информированным, сознательным и однозначным. Согласие на обработку ПДн может быть дано субъектом ПДн или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено законодательством Российской Федерации. В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются Министерством.

8.1.2. В случаях, когда в соответствии с требованиями законодательства обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн (в частности, при обработке ПДн специальных категорий). Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта ПДн на обработку его ПДн должно включать в себя, в частности:

фамилию, имя, отчество, адрес субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

фамилию, имя, отчество, адрес представителя субъекта ПДн, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта ПДн);

наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта ПДн;

цель обработки ПДн;

перечень ПДн, на обработку которых дается согласие субъекта ПДн;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка будет поручена такому лицу;

перечень действий с ПДн, на совершение которых дается согласие, общее описание используемых оператором способов обработки ПДн;

срок, в течение которого действует согласие субъекта ПДн, а также способ его отзыва, если иное не установлено федеральным законом;

подпись субъекта персональных данных.

8.1.3. Требования пункта 8.1.2 настоящего Положения не распространяются на случаи, когда письменная форма согласия субъекта ПДн на обработку его ПДн выбрана Министерством как оператором ПДн, но не является обязательной согласно требованиям законодательства Российской Федерации.

8.1.4. Согласие на обработку ПДн может быть отозвано субъектом ПДн. В случае отзыва субъектом ПДн согласия на обработку ПДн Министерство вправе продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, предусмотренных законодательством Российской Федерации.

8.1.5. Получение согласия на обработку ПДн осуществляется сотрудником при получении ПДн от субъекта ПДн путем оформления согласия по форме, установленной в приложении N 11 к настоящему распоряжению, за исключением случаев, указанных в пункте 8.1.2 настоящего Положения.

8.1.6. Если в соответствии с законодательством Российской Федерации предоставление ПДн и (или) получение Министерством согласия на обработку ПДн являются обязательными, Министерство обязано разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку.

8.2. Права субъекта в отношении ПДн, обрабатываемых Министерством.

8.2.1. Субъект ПДн имеет право:

получать от Министерства информацию, касающуюся обработки его ПДн в установленном законодательством Российской Федерации порядке. Сведения должны быть предоставлены субъекту ПДн в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта ПДн или его представителя в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн, за исключением случаев, если имеются законные основания для раскрытия таких ПДн. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Министерством в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Перечень сведений и порядок получения сведений предусмотрен законодательством Российской Федерации;

обращаться в Министерство по вопросу уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законодательством Российской Федерации меры по защите своих прав;

обращаться в Министерство с отзывом ранее данного Министерству согласия на обработку его ПДн. При этом такое обращение должно содержать информацию, на основании которой Министерство может однозначно определить субъекта ПДн и ПДн, на обработку которых субъект ПДн отзывает согласие;

давать предварительное письменное согласие при принятии Министерством исключительно в процессе автоматизированной обработки ПДн решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих его права и законные интересы;

заявлять возражения на решения Министерства в процессе исключительно автоматизированной обработки ПДн и на возможные юридические последствия таких решений;

обжаловать действия или бездействие Министерства в уполномоченный орган по защите прав субъектов ПДн или в судебном порядке.

8.3. Права и обязанности Министерства при обработке ПДн.

8.3.1. Министерство вправе:

поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия соответствующего акта, в порядке, предусмотренном законодательством Российской Федерации;

в случае отзыва субъектом ПДн согласия на обработку ПДн продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, предусмотренных законодательством Российской Федерации;

отказать субъекту ПДн в выполнении повторного запроса сведений, не соответствующего условиям, предусмотренным законодательством Российской Федерации. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Министерстве;

самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Министерства, предусмотренных законодательством Российской Федерации;

делегировать отдельные функции по обработке и защите ПДн подведомственным Министерству учреждениям, с учетом требований законодательства Российской Федерации.

8.3.2. Министерство обязано:

до начала обработки ПДн уведомить уполномоченный орган по защите прав субъектов ПДн о

своем намерении осуществлять обработку ПДн;

назначить должностное лицо, ответственное за организацию обработки ПДн;

при сборе ПДн, в том числе посредством информационно-телекоммуникационной сети Интернет, обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных законодательством Российской Федерации;

разъяснить субъекту ПДн юридические последствия отказа предоставить его ПДн и (или) дать согласие на их обработку, если предоставление ПДн и (или) получение Министерством согласия на обработку ПДн являются обязательными;

при получении доступа к ПДн не раскрывать третьим лицам и не распространять ПДн без согласия субъекта ПДн, если иное не предусмотрено законодательством Российской Федерации;

представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований обработки ПДн без согласия субъекта ПДн;

до начала осуществления трансграничной передачи ПДн убедиться в том, что иностранным государством, на территорию которого осуществляется передача ПДн, обеспечивается адекватная защита прав субъектов ПДн;

разъяснить субъекту ПДн порядок принятия решения на основании исключительно автоматизированной обработки его ПДн и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом ПДн своих прав и законных интересов;

при сборе ПДн предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством Российской Федерации;

опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему политику Министерства в отношении обработки ПДн, к сведениям о реализуемых требованиях к защите ПД;

принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей Министерства, предусмотренных законодательством Российской Федерации;

представить документы и локальные акты, предусмотренные законодательством Российской Федерации, и (или) иным образом подтвердить принятие мер, необходимых и достаточных для обеспечения выполнения обязанностей Министерства по запросу уполномоченного органа по защите прав субъектов ПДн;

при обработке ПДн принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн;

ознакомить служащих Министерства, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику Министерства в отношении обработки ПДн, локальными актами Министерства по вопросам обработки ПДн;

исполнять иные обязанности, предъявляемые к операторам ПДн законодательством Российской Федерации.

8.4. Хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", договором, стороной которого является субъект ПДн.

8.5. Особенности трансграничной передачи ПДн.

8.5.1. До начала осуществления деятельности по трансграничной передаче ПДн Министерство обязано уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять трансграничную передачу ПДн. Указанное уведомление направляется отдельно от уведомления о намерении осуществлять обработку ПДн, предусмотренного статьей 22 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

8.5.2. До подачи уведомления, предусмотренного пунктом 8.5.1, Министерство обязано получить от органов власти иностранного государства, иностранных физических лиц, иностранных юридических лиц, которым планируется трансграничная передача ПДн, следующие сведения:

сведения о принимаемых ими мерах по защите передаваемых ПДн и об условиях прекращения их обработки;

информация о правовом регулировании в области ПДн иностранного государства, под юрисдикцией которого они находятся (в случае, если предполагается осуществление трансграничной передачи ПДн органам власти иностранного государства, иностранным физическим лицам, иностранным юридическим лицам, находящимся под юрисдикцией иностранного государства, не являющегося стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн и не включенного в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов ПДн);

сведения об органах власти иностранного государства, иностранных физических лицах, иностранных юридических лицах, которым планируется трансграничная передача ПДн (наименование либо фамилия, имя и отчество, а также номера контактных телефонов, почтовые адреса и адреса электронной почты).

В целях оценки достоверности сведений, содержащихся в уведомлении Министерства о своем намерении осуществлять трансграничную передачу ПДн, перечисленные сведения предоставляются Министерством по запросу уполномоченного органа по защите прав субъектов ПДн в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Министерством в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

8.5.3. Трансграничная передача ПДн может быть запрещена или ограничена в целях защиты основ конституционного строя Российской Федерации, нравственности, здоровья, прав и законных интересов граждан, обеспечения обороны страны и безопасности государства, защиты экономических и финансовых интересов Российской Федерации, обеспечения дипломатическими и международно-правовыми средствами защиты прав, свобод и интересов граждан Российской Федерации, суверенитета, безопасности, территориальной целостности Российской Федерации и других ее интересов на международной арене с даты принятия уполномоченным органом по защите прав субъектов ПДн решения о запрещении или об ограничении трансграничной передачи ПДн, которое принимается уполномоченным органом по защите прав субъектов персональных данных по результатам рассмотрения уведомления, предусмотренного пунктом 8.5.1.

В случае принятия уполномоченным органом по защите прав субъектов персональных данных решения о запрещении или об ограничении трансграничной передачи ПДн Министерство обязано обеспечить уничтожение органом власти иностранного государства, иностранным физическим лицом, иностранным юридическим лицом ранее переданных им ПДн.

8.5.4. В случаях, предусмотренных законодательством Российской Федерации, требования пунктов 8.5.1 - 8.5.3 не применяются к вопросам трансграничной передачи Министерством ПДн в целях выполнения возложенных международным договором Российской Федерации, законодательством Российской Федерации на него функций, полномочий и обязанностей.

8.6. В целях информационного обеспечения в Министерстве могут создаваться специализированные справочники (телефонные, адресные книги и др.), содержащие ПДн, к которым с письменного согласия субъекта ПДн может предоставляться доступ неограниченному кругу лиц. Сведения о субъекте ПДн должны быть незамедлительно исключены из общедоступных источников ПДн по требованию субъекта ПДн либо по решению суда или иных уполномоченных государственных органов.

9. Ответственность за нарушение законодательства в области обработки и защиты ИОД, обработки и защиты ПДн

9.1. Руководители Министерства и руководители структурных подразделений Министерства несут ответственность за необеспечение конфиденциальности ИОД, за несоблюдение прав и свобод субъектов ПДн в отношении их ПДн, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

9.2. Сотрудники Министерства несут персональную ответственность за несоблюдение требований по обработке и обеспечению безопасности ИОД, установленных настоящим Положением, в соответствии с законодательством Российской Федерации.

9.3. Сотрудник Министерства может быть привлечен к ответственности в случаях:

умышленного или неумышленного раскрытия либо искажения ИОД;

утраты материальных носителей ИОД;

нарушения требований настоящего Положения и других нормативных документов Министерства в части вопросов доступа и работы с ИОД;

нарушения установленного порядка обработки и обеспечения безопасности ИОД, несанкционированного доступа к ИОД, раскрытия ИОД и нанесения Министерству, его сотрудникам, клиентам, субъектам обрабатываемых в Министерстве ПДн материального или морального ущерба.

Приложение N 3
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПОЛОЖЕНИЕ
О ПОРЯДКЕ УЧЕТА, ХРАНЕНИЯ И ОБРАЩЕНИЯ СО СЪЕМНЫМИ НОСИТЕЛЯМИ ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

1. Общие положения

Настоящее Положение о порядке учета, хранения и обращения со съемными носителями персональных данных и иной информации ограниченного доступа разработано в соответствии с федеральными законами от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 21 марта 2012 г. N 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", Требованиями о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств, утвержденными приказом ФСБ России от 24 октября 2022 г. N 524, Инструкцией по делопроизводству в исполнительных органах государственной власти Московской области, государственных органах Московской области, утвержденной постановлением Губернатора Московской области от 21 июня 2022 г. N 201-ПГ, и устанавливает порядок учета и использования машинных носителей информации для обработки информации ограниченного доступа (далее - ИОД), в том числе персональных данных (далее - ПДн).

Действие настоящего Положения о распространяется на всех сотрудников Министерства, подведомственных ему организаций, подрядчиков и представителей третьей стороны, имеющих доступ к информации ограниченного доступа, обрабатываемой в Министерстве.

2. Основные термины, сокращения и определения

АРМ - автоматизированное рабочее место пользователя (персональный компьютер (ПК) с прикладным ПО) для выполнения определенной производственной задачи.

ИБ - информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИС (ИСПДн) - информационная система (персональных данных).

ИОД - информация, доступ к которой ограничен законодательством Российской Федерации.

МНИ - материальный носитель, используемый для хранения и передачи электронной информации.

МНИ ОД - съемный МНИ, предназначенный для обработки ПДн либо другой ИОД.

ПК - персональный компьютер.

ПО - программное обеспечение вычислительной техники.

ПО вредоносное - ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.

3. Порядок использования машинных носителей информации

3.1. Под использованием МНИ ОД в ИС понимается их подключение к инфраструктуре ИС с целью обработки ПДн либо другой ИОД и обмена информацией между ИС и МНИ ОД.

3.2. В ИС для обработки ИОД допускается использование только учтенных МНИ ОД, которые являются собственностью Министерства и подвергаются регулярной ревизии и контролю.

3.3. К МНИ ОД предъявляются требования ИБ в соответствии с классами (уровнями) защищенности АРМ, для работы с которыми они предназначены. Целесообразность применения дополнительных мер обеспечения ИБ определяется администраторами ИС.

3.4. Не допускается подключение МНИ ОД, содержащих ИОД, к АРМ (ИС), не предназначенным для обработки ИОД (не имеющим подтверждающих соответствие требованиям ИБ для обработки ИОД документов, например - аттестатов соответствия требованиям ИБ).

4. Порядок учета, хранения и обращения со съемными машинными носителями персональных данных

4.1. Все находящиеся на хранении и в обращении МНИ ОД подлежат учету.

4.2. Каждый МНИ ОД должен иметь уникальный учетный номер.

4.3. Учет и выдача МНИ ОД осуществляются уполномоченными сотрудниками структурных подразделений Министерства, назначенными соответствующими приказами. Факт выдачи МНИ ОД пользователю фиксируется в журнале учета МНИ ОД (приложение N 18 к настоящему распоряжению) (далее - Журнал).

4.4. Пользователи получают учтенные МНИ ОД от уполномоченных сотрудников структурных подразделений Министерства на время выполнения соответствующих работ, по окончании которых данные носители подлежат возврату. Факты выдачи и возврата МНИ ОД фиксируются в Журнале.

4.5. При использовании пользователями МНИ ОД необходимо:

соблюдать требования настоящего Положения;

использовать МНИ ОД исключительно для выполнения своих служебных обязанностей;

ставить в известность администраторов ИС о любых фактах нарушения требований настоящего Положения;

бережно относится к МНИ ОД;

обеспечивать безопасность МНИ ОД;

извещать администраторов ИС о фактах утраты (кражи) МНИ ОД.

4.6. При использовании МНИ ОД запрещается:

использовать их в личных целях;

передавать их другим лицам (за исключением передачи МНИ ОД в целях, предусмотренных служебной необходимостью, при условии соблюдения требований информационной безопасности и учета МНИ ОД);

хранить их вместе с общедоступными данными на (в) рабочих столах либо оставлять без присмотра или передавать на хранение другим лицам;

подключать МНИ ОД, содержащие ИОД, к АРМ (ИС), не предназначенных для обработки ИОД;

выносить их из служебных помещений для работы на дому.

4.7. Обработка, прием и передача ПДн (ИОД), инициированные сотрудником между ИС и неучтенными МНИ, рассматриваются как несанкционированные. Администратор ИС оставляет за собой право блокировать или ограничивать использование МНИ ОД.

4.8. В случае выявления фактов несанкционированного и (или) нецелевого использования МНИ ОД инициируется служебная проверка, проводимая комиссией, состав и полномочия которой

определяется ответственным за обеспечение информационной безопасности в Министерстве. По результатам служебной проверки составляется акт расследования инцидента (приложение N 19 к настоящему распоряжению) и передается руководителю структурного подразделения для принятия мер в соответствии с законодательством Российской Федерации.

4.9. Информация, хранящаяся на МНИ ОД, подлежит обязательной проверке на предмет отсутствия вредоносного ПО, в соответствии с политикой антивирусной защиты, действующей в Министерстве.

4.10. При отправке или передаче ПДн (ИОД) адресатам на МНИ ОД записываются только предназначенные им данные. Отправка ПДн (ИОД) адресатам на МНИ ОД осуществляется в порядке, установленном для документов с пометкой "Для служебного пользования".

4.11. Вынос МНИ ОД для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения либо согласования (подписания) им сопроводительного письма, к которому прилагается МНИ ОД.

4.12. Если в соответствии с технологическим процессом обработки ИОД (ПДн) в ИС несанкционированных доступ к МНИ ОД не может быть исключен, для защиты такой информации должны применяться сертифицированные ФСБ России средства криптографической защиты информации (далее - СКЗИ).

4.13. В случае утраты или несанкционированного уничтожения МНИ ОД либо разглашения содержащихся на них сведений немедленно ставится в известность руководитель соответствующего структурного подразделения. По факту утраты составляется акт расследования инцидента и в журналы учета носителей ОД вносятся соответствующие отметки.

4.14. МНИ ОД, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

4.15. В случае увольнения или перевода сотрудника в другое структурное подразделение предоставленные ему МНИ ОД необходимо сдать уполномоченному лицу структурного подразделения. Уполномоченное лицо должно предпринять одно из следующих мер, направленных на невозможность несанкционированного доступа хранящейся на нем защищаемой информации:

уничтожить МНИ ОД с составлением соответствующего акта;

удалить информацию, содержащуюся на МНИ ОД, с составлением соответствующего акта;

сдать в архив или перерегистрировать МНИ ОД на структурное подразделение и сделать соответствующую отметку в Журнале.

5. Особенности эксплуатации носителей аутентифицирующей и парольной информации средств криптографической защиты информации

5.1. В помещениях, в которых размещены и (или) хранятся носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - МНИ СКЗИ), должен

обеспечиваться режим, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в такие помещения, который достигается посредством:

утверждения правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

утверждения перечня лиц, имеющих право доступа в помещения.

5.2. Помещения, в которых размещены и (или) хранятся МНИ СКЗИ, предназначенные для защиты информации, содержащейся в ИС (сегмента ИС), предназначенной для решения задач ИС на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации, обрабатывающей информацию высокого уровня значимости, должны соответствовать следующим требованиям:

окна помещений, расположенных на первых и (или) последних этажах зданий, а также окна помещений, находящихся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения;

окна и двери помещений, в которых размещены серверы ИС, должны быть оборудованы металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.

6. Ответственность

Пользователи и администраторы ИС, а также иные сотрудники Министерства, нарушившие требования настоящего Положения, несут ответственность в соответствии с законодательством Российской Федерации.

Приложение N 4
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПРАВИЛА
РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей (далее - Правила, ПДн, соответственно) определяют порядок учета (регистрации),

рассмотрения обращений либо запросов субъектов ПДн или их представителей (далее - запросы), подготовки ответов на запросы.

2. Настоящие Правила разработаны в соответствии федеральными законами от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Федеральный закон), от 2 мая 2006 г. N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", постановлениями Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации", от 21 марта 2012 г. N 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", Требованиями к подтверждению удаления персональных данных, утвержденными приказом Роскомнадзора от 28.10.2022 N 179.

3. Рассмотрение запросов о получении информации, касающейся обработки ПДн, и об уточнении ПДн субъекта, обрабатываемых в Министерстве, а также о блокировании, уничтожении неправомерно полученных (обрабатываемых) ПДн в Министерстве.

3.1. Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

подтверждение факта обработки ПДн в Министерстве;

правовые основания и цели обработки ПДн;

цели и применяемые в Министерстве способы обработки ПДн;

наименование и место нахождения Министерства как оператора ПДн, сведения о лицах (за исключением сотрудников Министерства), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн;

обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения (если иной порядок представления таких данных не предусмотрен законодательством Российской Федерации);

сроки обработки и хранения ПДн;

порядок осуществления субъектом ПДн своих прав как субъекта ПДн;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование организации или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению Министерства, если обработка поручена или будет поручена такому лицу;

информацию о способах исполнения Министерством обязанностей оператора ПДн;

иные сведения, предусмотренные законодательством Российской Федерации.

3.2. Должностные лица Министерства обеспечивают:

объективное, всестороннее и своевременное рассмотрения запроса;

принятие мер, направленных на восстановление или защиту нарушенных прав, свобод и законных интересов субъектов ПДн;

направление письменных ответов по существу запроса.

3.3. Сведения, указанные в пункте 3.1, предоставляются субъекту ПДн или его представителю Министерством в течение десяти рабочих дней с момента обращения либо получения Министерством запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Министерством в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.4. Запрос должен содержать:

номер основного документа, удостоверяющего личность субъекта ПДн или его представителя;

сведения о дате выдачи указанного документа и выдавшем его органе;

сведения, подтверждающие участие субъекта ПДн в отношениях с Министерством либо сведения, иным образом подтверждающие факт обработки ПДн Министерством;

подпись субъекта ПДн или его представителя.

Запрос может быть направлен в форме электронного документа и подписан ЭП в соответствии с законодательством Российской Федерации.

3.5. Министерство предоставляет сведения, указанные в пункте 3.1, субъекту ПДн или его представителю в той форме, в которой направлены соответствующий запрос, если иное не указано в запросе.

3.6. Министерство обязано сообщить субъекту ПДн или его представителю информацию о наличии ПДн, относящихся к соответствующему субъекту ПДн, а также предоставить возможность ознакомления с этими ПДн при обращении субъекта ПДн или его представителя в течение десяти рабочих дней с даты получения запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Министерством в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

Министерство обязано предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к нему.

3.7. В случае если сведения, указанные в пункте 3.1, либо обрабатываемые ПДн, были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе направить повторный запрос в целях получения таких сведений (ознакомления с такими ПДн) не ранее чем через тридцать дней после первоначального запроса, если более короткий срок не установлен

законодательством Российской Федерации или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

Субъект ПДн вправе повторно направить запрос в Министерство в целях получения сведений (ознакомления с обрабатываемыми ПДн) до истечения указанного выше срока в случае, если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального запроса. Повторный запрос наряду со сведениями, указанными в пункте 3.3, должен содержать обоснование направления повторного запроса.

Запрос рассматривается должностными лицами Министерства, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской.

Министерство вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего перечисленным условиям. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Министерстве.

3.8. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии с законодательством Российской Федерации, в том числе если:

обработка ПДн, включая ПДн, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

3.9. Субъект ПДн вправе обращаться в Министерство в целях уточнения его ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, уполномоченные должностные лица Министерства обязаны внести в них необходимые изменения.

В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные должностные лица Министерства обязаны уничтожить такие ПДн с оформлением акта уничтожения ПДн (приложение N 14 к настоящему распоряжению).

Министерство обязано уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы.

3.10. В целях обработки запросов Министерство вправе запрашивать информацию, требуемую для ответа за запрос, у организаций, которые участвуют в обработке ПДн субъекта ПДн на основании поручения Министерства либо иных предусмотренных законодательством Российской Федерации основаниях.

3.11. В случае отказа в предоставлении ПДн или информации о наличии ПДн о соответствующем субъекте ПДн субъекту ПДн или его представителю при их обращении либо при получении запроса уполномоченные должностные лица Министерства обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положения законодательства Российской Федерации, являющиеся основанием для такого отказа, в срок, не превышающий десяти рабочих дней со дня обращения субъекта ПДн или его представителя либо с даты получения запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Министерством в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.12. В случае выявления неправомерной обработки ПДн при обращении субъекта ПДн или его представителя, либо по запросу субъекта ПДн или его представителя, либо уполномоченного органа по защите прав субъектов ПДн уполномоченные должностные лица Министерства обязаны осуществить блокирование неправомерно обрабатываемых ПДн, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки.

3.13. В случае выявления неточных ПДн при обращении субъекта ПДн или его представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов ПДн, уполномоченные должностные лица Министерства обязаны осуществить блокирование ПДн, относящихся к этому субъекту ПДн, с момента такого обращения или получения указанного запроса на период проверки, если блокирование ПДн не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

3.14. В случае подтверждения факта неточности ПДн уполномоченные должностные лица Министерства на основании сведений, представленных субъектом ПДн или его представителем, либо уполномоченным органом по защите прав субъектов ПДн, или иных необходимых документов, обязаны уточнить ПДн в течение семи рабочих дней со дня представления таких сведений и снять блокирование ПДн.

3.15. В случае выявления неправомерной обработки ПДн уполномоченные должностные лица Министерства в срок, не превышающий трех рабочих дней с даты этого выявления, обязаны прекратить неправомерную обработку ПДн. В случае если обеспечить правомерность обработки ПДн невозможно, уполномоченные должностные лица Министерства в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязаны уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении ПДн Министерство обязано уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

3.16. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, Министерство обязано с момента выявления такого инцидента уведомить уполномоченный орган по защите прав субъектов ПДн:

в течение двадцати четырех часов - о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном оператором на взаимодействие с уполномоченным органом по защите прав субъектов ПДн, по вопросам, связанным с выявленным инцидентом;

в течение семидесяти двух часов - о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

3.17. Министерство обязано сообщать в уполномоченный орган по защите прав субъектов ПДн по запросу этого органа необходимую информацию в течение десяти рабочих дней с даты получения такого запроса. Указанный срок может быть продлен, но не более чем на пять рабочих дней, в случае направления оператором в адрес уполномоченного органа по защите прав субъектов ПДн мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

3.18. В случае выявления инцидента, повлекшего неправомерную передачу (предоставление, распространение, доступ) ПДн, Министерство обязано в порядке, определенном ФСБ России, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о таких инцидентах.

3.19. Взаимодействие Министерства с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн, осуществляется через Национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ) в соответствии с подпунктом 4.8 пункта 4 Положения о НКЦКИ.

3.20. Подтверждением передачи Министерством в НКЦКИ информации, указанной в п. 5.1

настоящей Инструкции, является присвоение НКЦКИ соответствующим компьютерным инцидентам идентификаторов. Идентификаторы направляются НКЦКИ в Министерство по тем же каналам, по которым Министерством была направлена информация о соответствующем инциденте в НКЦКИ.

3.21. Рассмотрение запросов является служебной обязанностью уполномоченных должностных лиц, в чьи обязанности входит обработка ПДн, а также должностного лица, ответственного за рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей. При необходимости к обработке запросов могут привлекаться представители организаций, подведомственных Министерству, при условии соблюдения требований законодательства Российской Федерации.

3.22. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

4. Рассмотрение отзывов согласий субъектов ПДн либо их представителей на обработку их ПДн в Министерстве.

4.1. В случае отзыва субъектом ПДн или его представителем согласия на обработку его ПДн (далее - отзыв согласия) Министерство обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Министерства) и в случае, если сохранение ПДн более не требуется для целей обработки ПДн, уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Министерства) в срок, не превышающий тридцати дней с даты регистрации указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации.

4.2. В случае обращения субъекта ПДн в Министерство с требованием о прекращении обработки ПДн Министерство обязано в срок, не превышающий десяти рабочих дней с даты получения соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если обработка ПДн осуществляется другим лицом, действующим по поручению Министерства), за исключением случаев, предусмотренных законодательством Российской Федерации. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Министерством в адрес субъекта ПДн мотивированного уведомления с указанием причин продления срока.

4.3. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в пунктах 4.1 и 4.2, Министерство осуществляет блокирование таких ПДн или обеспечивает их блокирование (если обработка ПДн осуществляется другим лицом, действующим по поручению Министерства) и обеспечивает уничтожение ПДн в срок не более чем шесть месяцев, если иной срок не установлен законодательством Российской Федерации.

4.4. Отзыв согласия, данного Министерству, либо требование о прекращении обработки ПДн Министерством, осуществляется посредством обращения либо направления запроса субъекта ПДн или его представителя в Министерство.

4.5. Отзыв согласия, данного организации, по поручению которой Министерство осуществляет обработку ПДн, либо требование о прекращении обработки ПДн такой организацией, осуществляется посредством обращения либо направления запроса субъекта ПДн или его представителя в такую организацию, которая после получения запроса (обращения) обеспечивает прекращение обработки ПДн в Министерстве посредством направления в Министерство информации о полученном обращении (запросе).

4.6. Регистрация запроса (обращения) субъекта ПДн либо письма с информацией о наличии запроса (обращения) от организации, в которую обратился субъект ПДн, осуществляется в соответствии с Правилами делопроизводства, действующими в Министерстве, с учетом требования о соблюдении конфиденциальности информации, доступ к которой ограничен законодательством Российской Федерации. После регистрации запрос (обращение, письмо) в установленном в Министерстве порядке направляется для дальнейшего рассмотрения лицу, ответственному за рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей.

4.7. Порядок действий в случае принятия решения о необходимости удаления ПДн субъекта ПДн.

4.7.1. В случае принятия решения о необходимости удаления ПДн субъекта ПДн они подлежат удалению сотрудниками Министерства, имеющими соответствующие полномочия по доступу к ИСПДн Министерства. При необходимости к процессу удаления ПДн из ИС Министерства могут привлекаться представители организаций, подведомственных Министерству, при условии соблюдения требований законодательства Российской Федерации.

4.7.2. После удаления ПДн оформляется акт уничтожения ПДн в соответствии с формой (приложение N 14 к настоящему распоряжению). Акт уничтожения ПДн подписывается Комиссией в составе:

глава комиссии - должностное лицо, ответственное за обеспечение информационной безопасности в Министерстве, либо должностное лицо, ответственное за организацию обработки ПДн в Министерстве;

члены комиссии - должностные лица, ответственные за функционирование ИС, из которых осуществляется удаление ПДн, должностные лица, обеспечившие уничтожение ПДн, а также должностное лицо, ответственное за рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей.

4.7.3. Акт уничтожения ПДн подписывается членами комиссии собственноручно либо посредством квалифицированной электронной подписи в государственной информационной системе "Межведомственная система электронного документооборота".

4.7.4. Акт уничтожения ПДн в электронной форме, подписанный посредством квалифицированной электронной подписи в государственной информационной системе "Межведомственная система электронного документооборота", признается электронным документом, равнозначным акту уничтожения ПДн на бумажном носителе, подписанному собственноручной подписью членов комиссии.

4.7.5. Акты уничтожения ПДн хранятся у должностного лица, ответственного за рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей, на бумажном носителе либо в электронной форме.

4.7.6. Копия акта уничтожения ПДн, удаленных по результатам рассмотрения запроса (обращения) субъекта ПДн или его представителя в Министерство, а также информация об удалении ПДн, направляется субъекту ПДн либо его представителю в ответ на соответствующий запрос (обращение) в установленном в Министерстве порядке.

4.7.7. Копия акта уничтожения ПДн, удаленных по результатам рассмотрения письма от организации, в которую субъект ПДн или его представитель обращался по вопросам предоставления согласия Министерству на обработку его ПДн и (или) отзыва такого согласия, а также информация об удалении ПДн, направляется в указанную организацию в ответ на соответствующее письмо в установленном в Министерстве порядке, в целях уведомления указанной организацией субъекта ПДн информации об удалении ПДн Министерством.

4.7.8. В случае если обработка подлежащих удалению ПДн осуществляется с использованием средств автоматизации, кроме акта об уничтожении ПДн производится выгрузка из журнала регистрации событий в ИС. Выгрузка из журнала регистрации событий должна содержать:

фамилию, имя, отчество (при наличии) субъекта (субъектов) ПДн или иную информацию, относящуюся к субъекту ПДн, чьи ПДн были уничтожены;

перечень категорий уничтоженных ПДн субъекта ПДн;

наименование ИСПДн, из которой были уничтожены ПДн;

причину уничтожения ПДн;

дату уничтожения ПДн.

Если выгрузка из журнала не позволяет указать отдельные из перечисленных выше сведений, недостающие сведения вносятся в акт об уничтожении ПДн.

4.7.9. Акт уничтожения ПДн, а также (при наличии) выгрузка из журнала регистрации событий в ИСПДн, подлежат хранению в течение 3 лет с момента уничтожения ПДн.

4.7.10. В случае если ПДн, подлежащие удалению, при обработке в Министерстве были переданы третьим лицам (организациям), Министерство обязано уведомить указанных лиц (организации) об отзыве согласия и обеспечить удаление ПДн, обрабатываемых данными лицами (организации).

4.7.11. Действие п. 4.7.10 Правил не распространяется на случаи передачи ПДн третьим лицам (организациям), не предусматривающие необходимость согласия субъекта ПДн на такую передачу.

4.8. Порядок действий в случае принятия решения о невозможности удаления ПДн субъекта ПДн на основании отзыва им (его представителем) согласия на обработку ПДн.

4.8.1. Министерство вправе принять решение о невозможности удаления ПДн субъекта ПДн по результатам рассмотрения отзыва согласия или письма с информацией об отзыве согласия от организации, по поручению которой Министерство обрабатывает ПДн, в случаях:

отсутствия в Министерстве ПДн, согласие на обработку которых отозвано;

невозможности однозначной идентификации субъекта ПДн или однозначного определения ПДн, которые подлежат удалению, на основании информации, указанной в отзыве согласия;

наличия оснований для обработки Министерством соответствующих ПДн без согласия субъекта ПДн на их обработку;

если оператором ИС, отзыв согласия на обработку в которых рассматривается, является иная организация (не Министерство).

4.8.2. В случае принятия решения о невозможности удаления ПДн информация о принятом решении, а также его обоснование и (при необходимости) рекомендации субъекту о его дальнейших действиях в целях удаления его ПДн, направляется в адрес субъекта ПДн либо его представителя в ответ на соответствующий запрос (обращение) либо в адрес организации, в которую обратился субъект ПДн, в ответ на соответствующее письмо, в порядке, установленном в Министерстве.

4.8.3. В случае если отзыв согласия был направлен в Министерство организацией, в которую субъект ПДн или его представитель обращался по вопросам предоставления согласия Министерству на обработку его ПДн и (или) отзыва такого согласия, информация о принятом решении, а также его обоснование и (при необходимости) рекомендации субъекту о его дальнейших действиях в целях удаления его ПДн, направляется в адрес указанной организации в ответ на соответствующее письмо в установленном в Министерстве порядке.

4.9. В целях возможности определения, какие именно обрабатываемые в Министерстве ПДн подлежат удалению, при направлении отзыва согласия рекомендуется включать в его состав информацию, однозначно идентифицирующую субъекта ПДн (паспортные данные, СНИЛС) либо подлежащие удалению ПДн (номер заявки в МФЦ, имя учетной записи (логин) на региональном портале оказания государственных услуг, другие идентификаторы субъекта ПДн как пользователя ИСПДн и т.п.).

4.10. В случае если в отзыве согласия перечислены конкретные ПДн, на обработку которых отзывается согласие, удалению подлежат только эти ПДн субъекта.

В случае если в отзыве согласия указаны названия конкретных ИС, из которых требуется удалить ПДн, удалению подлежат ПДн субъекта, обрабатываемые в указанных ИС (при условии, что оператором этих систем является Министерство).

В прочих случаях удалению подлежат все ПДн субъекта, обрабатываемые в Министерстве на момент направления субъектом ПДн отзыва согласия.

4.11. ПДн, обработка которых Министерством в соответствии с законодательством Российской Федерации не требует наличия согласия субъекта ПДн, по результатам рассмотрения

соответствующего отзыва согласия, удалению не подлежат.

4.12. ПДн, поступившие в Министерство (обработка которых началась в Министерстве) после даты отзыва согласия, по результатам его рассмотрения удалению не подлежат.

4.13. Рассмотрение отзывов согласий, а также писем от организаций, по поручению которых Министерство обрабатывает ПДн либо в которые обратился субъект ПДн по вопросам обработки его ПДн в Министерстве, является служебной обязанностью уполномоченных должностных лиц, в чьи обязанности входит обработка ПДн, а также должностного лица, ответственного рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей. При необходимости к обработке отзывов согласий и к удалению ПДн из информационных систем Министерства могут привлекаться представители организаций, подведомственных Министерству, при условии соблюдения требований законодательства Российской Федерации.

4.14. Запрос (обращение) считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

5. Обработка обращений (запросов) субъектов ПДн, содержащих информацию, доступ к которой ограничен законодательством Российской Федерации, в Министерстве осуществляется с учетом требований информационной безопасности.

При необходимости внесения такой информации в ИС указанные ИС должны соответствовать требованиям, предъявляемым к обработке соответствующих типов информации ограниченного доступа (в частности, ПДн соответствующих категорий).

6. В случае выявления фактов неправомерной обработки ПДн в Министерстве либо иных нарушений, связанных с обработкой ПДн в Министерстве, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

7. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Результаты служебной проверки докладываются министру.

8. Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение N 5
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПРАВИЛА

ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА ТРЕБОВАНИЯМ К ЗАЩИТЕ ИНФОРМАЦИИ

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации (далее - Правила) в Министерстве государственного управления, информационных технологий и связи Московской области (далее - Министерство) определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области обработки информации ограниченного доступа, в том числе персональных данных (далее - ИОД, ПДн, соответственно), основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ИОД требованиям к защите информации.

1.2. Настоящие Правила разработаны на основании Федеральных законов от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27 июля 2006 г. N 152-ФЗ "О персональных данных" и в соответствии с частью 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", утвержденных постановлением Правительства Российской Федерации от 21 марта 2012 г. N 211.

1.3. Министерство использует информационные системы, предназначенные для обработки ИОД (далее - ИС) в целях реализации возложенных на Министерство задач, исполнения государственных функций и полномочий Министерства.

1.4. Министерство использует информационные системы персональных данных (далее - ИСПДн) для выполнения основных целей и задач обработки ПДн, указанных в приложении N 2 к настоящему распоряжению.

1.5. Пользователями ИС (далее - Пользователь) являются сотрудники Министерства, участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ИОД и имеющие доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее - СЗИ) ИС.

1.6. В целях реализации возложенных на Министерство задач, исполнение государственных функций и полномочий Министерства отдельные функции обработки ИОД могут осуществляться сотрудниками подведомственных Министерству учреждений, с учетом требований законодательства Российской Федерации. В данном случае права и обязанности указанных сотрудников, связанные с обработкой ИОД и описанные в настоящих Правилах соответствуют правам и обязанностям сотрудников Министерства.

1.7. Контрольные мероприятия по обеспечению безопасности ИОД, требуемого уровня защищенности ПДн и соблюдению условий использования СЗИ, а также соблюдению требований законодательства Российской Федерации по защите ИОД, обработке и защите ПДн в ИС Министерства (далее - Контрольные мероприятия) проводятся в следующих целях:

проверка выполнения требований организационно-распорядительной документации по защите информации в Министерстве и законодательства Российской Федерации и Московской области в области защиты информации, защиты и обработки ПДн;

оценка уровня осведомленности и знаний сотрудников Министерства в области защиты информации, защиты и обработки ПДн;

оценка обоснованности и эффективности применяемых мер и средств защиты ИОД.

2. Тематика внутреннего контроля соответствия обработки ИОД требованиям к защите информации

2.1. В Министерстве проводятся Контрольные мероприятия следующих видов:

регулярные;

плановые;

внеплановые.

2.2. Регулярные Контрольные мероприятия периодически проводятся в ИС (ИСПДн) Министерства администраторами ИС (ИСПДн) и предназначены для осуществления контроля выполнения требований в области защиты ИОД в Министерстве.

2.3. Плановые Контрольные мероприятия периодически проводятся Комиссией по проведению внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации Министерства (далее - Комиссия), состав которой утверждается правовым актом Министерства, не реже одного раза в год и направлены на постоянное совершенствование системы защиты информации в Министерстве.

2.4. Внеплановые Контрольные мероприятия проводятся на основании решения должностного лица, ответственного за защиту информации в Министерстве, созданной для проведения мероприятий комиссией (создается на период проведения мероприятий). Решение о проведении внеплановых Контрольных мероприятий может быть принято в следующих случаях:

по результатам расследования инцидента информационной безопасности;

по результатам внешних контрольных мероприятий, проводимых регулирующими органами в целях устранения выявленных замечаний;

в иных случаях по решению министра либо должностного лица, ответственного за защиту информации в Министерстве.

3. Планирование Контрольных мероприятий

3.1. Для проведения плановых Контрольных мероприятий должностное лицо, ответственное за выполнение работ по защите информации в Министерстве, утверждает план проведения внутреннего контроля условий обработки персональных данных (иной информации ограниченного

доступа) в Министерстве на текущий год, форма которого утверждается правовым актом Министерства.

3.2. Плановые Контрольные мероприятия в отношении ИОД, не содержащей ПДн, проводятся совместно с Контрольными мероприятиями в отношении ПДн.

3.3. Плановые Контрольные мероприятия осуществляются Комиссией в соответствии с программой (порядком) проведения внутреннего контроля соответствия обработки ПДн требованиям законодательства Российской Федерации, утверждаемой правовым актом Министерства.

4. Порядок проведения плановых и внеплановых Контрольных мероприятий

4.1. При проведении плановых и внеплановых Контрольных мероприятий Комиссия руководствуется Положением о комиссии по проведению внутреннего контроля соответствия обработки ПДн требованиям законодательства Российской Федерации, утверждаемым правовым актом Министерства.

4.2. Плановые и внеплановые Контрольные мероприятия проводятся Комиссией при участии лица, ответственного за обеспечение информационной безопасности в Министерстве. Также по его ходатайству к проведению Контрольных мероприятий могут привлекаться администраторы ИС и лица, ответственные за эксплуатацию ИС либо за обеспечение безопасности информации в ИС.

4.3. При необходимости к проведению Контрольных мероприятий могут привлекаться представители организаций, подведомственных Министерству, при условии соблюдения требований законодательства Российской Федерации.

4.4. Во время проведения контрольных мероприятий в зависимости от целей мероприятий могут выполняться следующие проверки:

оценка соответствия процессов обработки ИОД, в том числе ПДн, в Министерстве, требованиям законодательства Российской Федерации;

оценка достаточности локальных нормативных актов Министерства в области защиты ИОД, обработки и защиты ПДн, и их соответствия требованиям законодательства Российской Федерации в указанных областях;

соответствия полномочий пользователей ИС (ИСПДн) правилам доступа;

соблюдения пользователями требований законодательства Российской Федерации к обработке ПДн;

соблюдения пользователями требований законодательства Российской Федерации к защите ИОД;

соблюдения Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ИОД, иных локальных

нормативных актов Министерства в области обработки и защиты ИОД, обработки ПДн;

знания и соблюдения администраторами ИС инструкций и регламентов по обеспечению безопасности информации в Министерстве;

соблюдения порядка доступа сотрудников в помещения Министерства, где ведется обработка ИОД, в том числе ПДн (приложение N 13 к настоящему распоряжению);

порядок и условия применения средств защиты информации;

состояние учета машинных носителей ПДн (ИОД);

наличие (отсутствие) фактов несанкционированного доступа к ИОД и принятие необходимых мер;

проведенные мероприятия по восстановлению ИОД, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации, средств обработки и защиты информации;

проверки соблюдения других требований законодательства Российской Федерации, Московской области, локальных правовых актов Министерства в области защиты информации, защиты и обработки ПДн.

5. Оформление результатов контрольных мероприятий

5.1. По итогам проведения регулярных Контрольных мероприятий выявленные инциденты и нарушения (при их наличии) фиксируются в журнале учета событий информационной безопасности (приложение N 16 к распоряжению).

5.2. По итогам проведения плановых и внеплановых Контрольных мероприятий оформляется акт проведения контроля, форма которого утверждается правовым актом Министерства.

5.3. При наличии выявленных нарушений процесса обработки ПДн (ИОД) по результатам плановых и внеплановых Контрольных мероприятий оформляется план мероприятий по устранению выявленных нарушений, форма которого утверждается правовым актом Министерства.

5.4. Оформленные по результатам проведения плановых и внеплановых Контрольных мероприятий акт проведения контроля и план мероприятий по устранению выявленных нарушений подписываются членами Комиссии и утверждаются ее председателем.

5.5. Результаты проведения плановых и внеплановых Контрольных мероприятий доводятся до министра. Отчетные документы, оформленные по результатам проведения указанных мероприятий, при необходимости (в целях исполнения требований законодательства Российской Федерации либо по запросу) направляются в уполномоченные федеральные исполнительные органы государственной власти Российской Федерации в установленном в Министерстве порядке.

Приложение N 6
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПРАВИЛА
РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

1. Общие положения

Настоящие Правила работы с обезличенными данными разработаны с учетом Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Федеральный закон), приказа Роскомнадзора от 5 сентября 2013 г. N 996 "Об утверждении требований и методов по обезличиванию персональных данных" и постановления Правительства Российской Федерации от 21 марта 2012 г. N 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" и определяют порядок работы с обезличенными данными Министерства.

2. Термины и определения

В соответствии с Федеральным законом:

ПДн - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн);

обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн;

обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Условия обезличивания

Обезличивание ПДн может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых ПДн, снижения классов (требуемых уровней

защищенности) ИС (ИСПДн), а также проводиться в отношении ПДн по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено Федеральным законом.

К методам обезличивания ПДн относятся:

метод введения идентификаторов;

метод изменения состава или семантики;

метод декомпозиции;

метод перемешивания.

Перечень должностей сотрудников Министерства, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн, приведен в приложении N 7 к настоящему распоряжению;

решение о необходимости обезличивания ПДн принимает должностное лицо, ответственное за защиту информации в Министерстве либо должностное лицо, ответственное за обработку ПДн в Министерстве;

руководители структурных подразделений, непосредственно осуществляющие обработку ПДн, готовят предложения по обезличиванию ПДн, обоснование такой необходимости и способ обезличивания;

сотрудники подразделений, обслуживающих информационные системы (базы данных), содержащие ПДн, осуществляют непосредственное обезличивание выбранным способом.

4. Порядок работы с обезличенными ПДн

Обезличенные данные не подлежат разглашению и нарушению конфиденциальности, если иное не определено законодательством Российской Федерации.

При обработке обезличенных данных должны приниматься меры, препятствующие их несанкционированному деобезличиванию.

Обезличенные данные могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных данных необходимо обеспечивать соблюдение требований законодательства Российской Федерации и Московской области в области защиты информации, защиты и обработки ПДн.

Приложение N 7

к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ, ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Руководители структурных подразделений, ответственных за эксплуатацию ИСПДн в соответствии с локальными правовыми актами Министерства.

Приложение N 8
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ, ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

N п/п	Наименование должности	Категория персональных данных
1.	Сотрудники управления экономического планирования, правовой и кадровой работы	ПДн гражданских служащих и сотрудников структурных подразделений Министерства; ПДн категорий "общедоступные", "иные"
2.	Сотрудники подразделений Министерства, участвующих в реализации функций и полномочий Министерства, предусматривающих необходимость обработки ПДн, в том числе в процессах оказания государственных услуг, обработки обращений граждан, а также обеспечения информационной безопасности	ПДн гражданских служащих и сотрудников структурных подразделений Министерства, а также лиц, не являющихся сотрудниками Министерства; ПДн категорий "общедоступные", "иные"

3.	Сотрудники подразделений Министерства, являющиеся пользователями (либо обеспечивающие функционирование) государственной информационной системы Московской области "Портал государственных и муниципальных услуг (функций) Московской области"	ПДн лиц, не являющихся сотрудниками Министерства; ПДн категорий "специальные", "общедоступные", "иные"

Приложение N 9
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ИНСТРУКЦИЯ ДОЛЖНОСТНОГО ЛИЦА, ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В МИНИСТЕРСТВЕ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ МОСКОВСКОЙ ОБЛАСТИ

1. Общие положения

Инструкция должностного лица, ответственного за организацию обработки ПДн в Министерстве государственного управления, информационных технологий и связи Московской области (далее - Инструкция, Министерство, соответственно), разработана в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Федеральный закон), постановлением Правительства Российской Федерации от 21 марта 2012 г. N 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" и закрепляет обязанности, права и ответственность должностного лица, ответственного за организацию обработки ПДн в Министерстве.

Должностное лицо, ответственное за организацию обработки ПДн в Министерстве, назначается правовым актом Министерства.

Должностное лицо, ответственное за организацию обработки ПДн в Министерстве, в своей работе руководствуется Федеральным законом, настоящей Инструкцией, а также нормативными актами Министерства, регламентирующими вопросы обработки ПДн.

2. Обязанности должностного лица, ответственного

за организацию обработки персональных данных

Должностное лицо, ответственное за организацию обработки ПДн в Министерстве, обязано:

организовывать осуществление внутреннего контроля за соблюдением сотрудниками Министерства законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

доводить до сведения сотрудников положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

организовывать прием и обработку обращений и запросов субъектов ПДн или их представителей и осуществлять контроль приема и обработки указанных обращений и запросов.

3. Права должностного лица, ответственного за организацию обработки персональных данных

Должностное лицо, ответственное за организацию обработки ПДн в Министерстве, имеет право:

принимать решения в пределах своей компетенции;

требовать от сотрудников соблюдения действующего законодательства, а также нормативных актов Министерства о ПДн;

взаимодействовать с управлениями и иными структурными подразделениями Министерства по вопросам обработки ПДн.

4. Ответственность должностного лица, ответственного за организацию обработки ПДн

За ненадлежащее исполнение или неисполнение настоящей Инструкции, а также за нарушение требований законодательства в области обработки ПДн, должностное лицо, ответственное за организацию обработки ПДн в Министерстве, несет предусмотренную законодательством Российской Федерации ответственность.

Приложение N 10
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

Типовое обязательство

гражданского служащего (сотрудника), непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных (служебных) обязанностей

Я, Ф.И.О., должность, паспорт серия _____ N _____, выдан _____
_____
обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных (служебных) обязанностей, в случае расторжения со мной служебного контракта, освобождения меня от замещаемой должности и увольнения с Федеральной государственной гражданской службы, прекращения (расторжения) трудового договора.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных сотрудника, или их утраты я несу ответственность в соответствии со статьями 15 и 42 Федерального закона от 27 июля 2004 г. N 79-ФЗ "О государственной гражданской службе Российской Федерации", статьей 90 Трудового кодекса Российской Федерации от 30 декабря 2001 г. N 197-ФЗ.

С Положением по обработке и защите информации ограниченного доступа, не составляющей государственную тайну, включая персональные данные, в Министерстве государственного управления, информационных технологий и связи Московской области ознакомлен(а).

_____ _____ _____
(должность) (подпись)
(Ф.И.О.)

_____
(дата)

Приложение N 11
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ТИПОВЫЕ ФОРМЫ СОГЛАСИЙ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Типовая форма согласия сотрудника на обработку персональных данных

СОГЛАСИЕ
сотрудника на обработку персональных данных

Я, _____,
(Ф.И.О. сотрудника)
зарегистрированный(ая) по адресу:
_____
_____
паспорт: серия _____, N _____, выдан
_____,
в соответствии со ст. 9 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" даю согласие на обработку своих персональных данных Мингосуправления Московской области, расположенному по адресу: Московская область, г. Красногорск, бульвар Строителей, д. 1, а именно: совершение действий, предусмотренных п. 3 ст. 3 Федерального закона N 152-ФЗ со всеми данными, которые находятся в распоряжении Мингосуправления Московской
области с целью начисления заработной платы, исчисления и уплаты
предусмотренных законодательством Российской Федерации налогов, сборов и взносов на обязательное социальное и пенсионное страхование, представления органом установленной законодательством отчетности в отношении физических лиц, в том числе сведений персонифицированного учета в Пенсионный фонд Российской Федерации, сведений подоходного налога в ФНС Российской
Федерации, сведений в ФСС Российской Федерации, предоставлять сведения в банк для оформления банковской карты и перечисления заработной платы на карты, и третьим лицам для оформления полиса ДМС, а также предоставлять сведения в случаях, предусмотренных федеральными законами и иными
нормативно-правовыми актами, следующих моих персональных данных:

1. Перечень персональных данных, на обработку которых дается согласие:

фамилия, имя, отчество (в т.ч. предыдущие), паспортные данные или данные документа, удостоверяющего личность, дата рождения, место рождения, гражданство, отношение к воинской обязанности и иные сведения военного билета и приписного удостоверения, данные документов о профессиональном образовании, профессиональной переподготовки, повышении квалификации, стажировке, данные документов о подтверждении специальных знаний, данные документов о присвоении ученой степени, ученого звания, списки научных трудов и изобретений и сведения о наградах и званиях, знание иностранных языков, семейное положение и данные о составе и членах семьи, сведения о социальных льготах, пенсионном обеспечении и страховании, данные документов об инвалидности (при наличии), данные медицинского заключения (при необходимости), стаж работы и другие данные трудовой книжки и вкладыша к трудовой книжке;

должность, квалификационный уровень, сведения о заработной плате (доходах), банковских счетах, картах, адрес места жительства (по регистрации и фактический), дата регистрации по указанному месту жительства, номер телефона (стационарный домашний, мобильный);

данные свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации (ИНН), данные страхового свидетельства государственного пенсионного страхования, данные страхового медицинского полиса обязательного страхования граждан.

2. Перечень действий, на совершение которых дается согласие:

разрешаю Мингосуправления Московской области производить с моими персональными данными действия (операции), определенные статьей 3 Федерального закона от 27 июля 2006 г. N 152-ФЗ, а именно: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных. Обработка персональных данных может осуществляться как с использованием средств автоматизации, так и без их использования (на бумажных носителях).

3. Согласие на передачу персональных данных третьим лицам:

разрешаю обмен (прием, передачу, обработку) моих персональными данных между Мингосуправления Московской области и третьими лицами в соответствии с заключенными договорами и соглашениями, в целях соблюдения моих законных прав и интересов.

4. Сроки обработки и хранения персональных данных:

обработка персональных данных прекращается по истечении семи лет после окончания трудового договора сотрудника. В дальнейшем бумажные носители персональных данных находятся на архивном хранении (постоянно или 75 лет), а персональные данные сотрудников на электронных носителях удаляются из информационной системы.

Согласие на обработку данных (полностью или частично) может быть отозвано субъектом персональных данных на основании его письменного заявления.

Права и обязанности в области защиты персональных данных мне разъяснены.

Настоящее согласие действует с "__" _____ 20__ г.

_____/_____/"__" _____ 20__ г.
(подпись) Ф.И.О. сотрудника

2. Типовая форма согласия на обработку персональных данных
(для лиц, не являющихся сотрудниками Мингосуправления Московской области)

Согласие
на обработку персональных данных

Я, _____,
(фамилия, имя, отчество полностью)
зарегистрированный(ная) по адресу
_____
(адрес регистрации)
паспорт гражданина РФ серия _____ N _____, выдан
_____
(кем и когда выдан)
мобильный телефон
_____
адрес электронной почты
_____
настоящим подтверждаю свое согласие уполномоченным должностным

лицам Министерства государственного управления, информационных технологий и связи Московской области, а также иных исполнительных органов государственной власти Московской области, органов местного самоуправления Московской области и их подведомственных учреждений, многофункциональных центров предоставления государственных и муниципальных услуг в Московской области, на обработку персональных данных (в соответствии с определением обработки персональных данных, указанным в Федеральном законе от 27 июля 2006 г. N 152-ФЗ "О персональных данных") в целях оказания мне государственных и муниципальных услуг и обеспечения моих законных прав и интересов, а также на получение информационных писем от имени Губернатора Московской области и исполнительных органов государственной власти Московской области, на получение государственных и муниципальных услуг в проактивном (автоматическом) режиме без оформления заявления, в том числе получение уведомлений о статусе оказания услуги; на получение информации о наличии налоговой задолженности путем отправки информационных запросов в Федеральную налоговую службу; на осуществление действий, необходимых для регистрации и аутентификации единой учетной записи в Федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме"; на прием и обработку сообщений, поступающих в Единую систему приема и обработки сообщений по вопросам деятельности исполнительных органов государственной власти Московской области, органов местного самоуправления муниципальных образований Московской области.

Настоящее согласие действует до достижения целей обработки персональных данных, указанных в настоящем согласии. Заявитель может отозвать настоящее согласие путем направления письменного уведомления (в части согласия на совершение действий, необходимых для оказания государственной или муниципальной услуги - не ранее окончания срока получения государственной или муниципальной услуги). Отзыв не будет иметь обратной силы в отношении персональных данных, прошедших обработку до окончания срока получения соответствующей государственной или муниципальной услуги, если иное не указано в тексте отзыва согласия.

В подтверждение изложенного нижеподписавшийся подтверждает свое согласие на обработку своих персональных данных в соответствии с положениями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

_____
(подпись) (расшифровка подписи)

Документы принял _____ Подпись _____/_____/

3. Типовая форма согласия на обработку персональных данных специальных категорий для их обработки в государственной информационной системе Московской области "Портал государственных и муниципальных услуг (функций) Московской области" (заполняется собственноручно на бумажном носителе в медицинском учреждении)

СОГЛАСИЕ
субъекта на обработку персональных данных и на передачу оператором персональных данных третьим лицам

Я как субъект персональных данных _____,
(фамилия, имя, отчество (при наличии)
_____,
(дата, месяц, год рождения)
паспорт/_____: серия _____ N _____,
(иной документ, удостоверяющий личность)
_____
(кем и когда выдан)
проживающий(ая) по адресу: _____

(индекс и адрес)
зарегистрирован(а): _____,
(индекс и адрес)
гражданство _____,
контактный телефон(ы): _____, адрес электронной почты: _____,
в соответствии с пунктом 3 статьи 3, пунктом 6 части 1 статьи 6, статьей 9, пунктами 3 - 4 части 2 статьи 10 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", статьями 13, 94 Федерального закона от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" и в целях оказания мне, как пациенту, медицинских услуг, включая информирование меня о результатах их оказания, даю согласие оператору -
_____
(полное наименование, адрес, индекс медицинской организации)
на обработку (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 (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных) моих персональных данных, включающих: фамилию, имя, отчество (при наличии) (в том числе предыдущие в случае изменения), пол, дата, месяц и год рождения, место рождения, гражданство, адрес места регистрации, дата регистрации, адрес места жительства, реквизиты (номер, серия) паспорта (иного документа, удостоверяющего личность) (при наличии), сведения о дате выдачи и выдавшем его органе, номер полиса обязательного медицинского страхования (ОМС), страховой номер индивидуального лицевого счета (СНИЛС) (при наличии), анамнез, сведения о состоянии моего здоровья, диагноз, вид

оказанной мне медицинской помощи, условия оказания медицинской помощи, сроки оказания медицинской помощи, объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах, результат обращения за медицинской помощью, серию и номер выданного листка нетрудоспособности (при наличии), сведения о проведенных медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результатах, примененные клинические рекомендации.

Оператор имеет право:

1) на обработку моих персональных данных, если она:

необходима для защиты моей жизни, здоровья и иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение моего согласия невозможно;

осуществляется в медико-профилактических целях, в целях установления мне медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

2) вносить мои персональные данные в электронную базу данных государственной информационной системы "Единая медицинская информационно-аналитическая система Московской области" (далее - ЕМИАС), оператором которой является

_____,
(полное наименование, адрес, индекс оператора)

включать в списки (реестры) и отчетные формы, предусмотренные законодательством Российской Федерации и законодательством Московской области, обмен (прием и передачу) моими персональными данными между ЕМИАС и государственной информационной системой Московской области "Портал государственных и муниципальных услуг (функций) Московской области", оператором которой является

_____,
(полное наименование, адрес, индекс оператора)

_____,
(наименование информационной системы, полное наименование, адрес, индекс оператора)

_____
(наименование информационной системы, полное наименование, адрес, индекс оператора)

с обеспечением их (персональных данных) защиты от несанкционированного доступа, без специального уведомления меня об этом;

3) осуществлять обработку моих персональных данных следующими способами: на бумажных носителях, в информационных системах с использованием и без использования средств автоматизации, а также смешанным способом.

Я также даю оператору согласие на:

1) использование моих персональных данных в целях информирования меня с помощью средств связи путем пересылки мне sms-сообщений или письма на мой

адрес электронной почты: напоминание о записи меня на прием к врачу,
специалисту, напоминание о записи меня на прохождение исследования,
обследования, напоминание о записи меня в процедурный кабинет,
_____;
(указать иное)
2) предоставление сведений о фактах моего обращения за медицинской помощью, в том числе через регистратуру/приемное отделение, и о состоянии моего здоровья, диагнозе, а также в случаях неблагоприятного прогноза развития
1
моего заболевания следующим лицам :
_____
(фамилия, имя, отчество (при наличии) полностью, контактный телефон)
_____
(фамилия, имя, отчество (при наличии) полностью, контактный телефон)
Настоящее согласие дано мной добровольно и действует бессрочно.
Я как субъект персональных данных оставляю за собой право отозвать данное согласие посредством составления письменного заявления в произвольной
форме, которое может быть направлено мной в адрес оператора по почте
заказным письмом с уведомлением о вручении либо передано под расписку
представителю оператора.

Я ознакомлен(а) с положениями:

части 7 статьи 5 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных":

"7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом";

статьи 14 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных":

"Статья 14. Право субъекта персональных данных на доступ к его персональным данным

1. Субъект персональных данных имеет право на получение сведений, указанных в части 7 настоящей статьи, за исключением случаев, предусмотренных частью 8 настоящей статьи. Субъект персональных данных вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

2. Сведения, указанные в части 7 настоящей статьи, должны быть предоставлены субъекту персональных данных оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением

случаев, если имеются законные основания для раскрытия таких персональных данных.

3. Сведения, указанные в части 7 настоящей статьи, предоставляются субъекту персональных данных или его представителю оператором в течение десяти рабочих дней с момента обращения либо получения оператором запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. Оператор предоставляет сведения, указанные в части 7 настоящей статьи, субъекту персональных данных или его представителю в той форме, в которой направлены соответствующие обращение либо запрос, если иное не указано в обращении или запросе.

4. В случае если сведения, указанные в части 7 настоящей статьи, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

5. Субъект персональных данных вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в части 7 настоящей статьи, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в части 4 настоящей статьи, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в части 3 настоящей статьи, должен содержать обоснование направления повторного запроса.

6. Оператор вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 настоящей статьи. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

9.1) информацию о способах исполнения оператором обязанностей, установленных статьей 18.1 настоящего Федерального закона;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

8. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-разыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.".

Субъект персональных данных _____ _____
(подпись)
(инициалы, фамилия)
Дата дачи настоящего согласия:
"__" _____ 2___ г.

---

1 Заполняется по желанию субъекта персональных данных.

Приложение N 12
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

Типовая форма
разъяснения субъекту персональных данных юридических
последствий отказа предоставить свои персональные данные
либо дать согласие на их обработку

Уважаемый(ая), _____!
(инициалы субъекта персональных данных)

В соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" уведомляем Вас, что обязанность
предоставления Вами персональных данных установлена
_____
(реквизиты и наименование нормативных правовых актов)
_____
В соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных" уведомляем Вас, что обязанность
предоставления Вами согласия на обработку Ваших персональных данных
установлена:
_____
(реквизиты и наименование нормативных правовых актов)

_____

В случае отказа Вами предоставить свои персональные данные либо дать согласие на их обработку, Мингосуправления Московской области не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям:

_____

_____

(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

При обработке Ваших персональных в Мингосуправления Московской области в соответствии с законодательством в области персональных данных Вы имеете право:

на получение сведений о Мингосуправления Московской области, о месте его нахождения;

требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;

на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;

на обжалование действия или бездействия Мингосуправления Московской области в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;

на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

_____ _____

(дата) (фамилия, инициалы и подпись сотрудника)

Приложение N 13
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ПОРЯДОК
ДОСТУПА СОТРУДНИКОВ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ И ИНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

1. Настоящий Порядок доступа сотрудников Мингосуправления Московской области в

помещения, в которых ведется обработка персональных данных и иной информации ограниченного доступа (далее - Порядок, ПДн, ИОД, соответственно), разработан в соответствии с требованиями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 21 марта 2012 г. N 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".

2. Целью настоящего Порядка является исключение несанкционированного доступа к ПДн и к иной ИОД в Мингосуправления Московской области.

3. Сотрудники Мингосуправления Московской области, получившие доступ к ПДн и иной ИОД, обязаны принимать меры, препятствующие раскрытию такой информации третьим лицам, распространению ПДн без согласия субъектов ПДн, если иное не предусмотрено Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", а также не распространять ИОД, за исключением случаев, определенных законодательством Российской Федерации.

4. Обеспечение безопасности ИОД от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий достигается, в том числе, установлением правил доступа в помещения, где обрабатываются такая информация в ИС либо без использования средств автоматизации.

5. Для помещений, в которых обрабатывается ИОД, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей ИОД и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

При хранении материальных носителей ИОД должны соблюдаться условия, обеспечивающие сохранность персональных данных (информация ограниченного доступа) и исключающие несанкционированный доступ к ним.

6. В помещения, где размещены технические средства, позволяющие осуществлять обработку ИОД, а также хранятся указанные носители информации, допускаются только сотрудники Министерства и подведомственных Министерству организаций, получившие доступ к ИОД, за исключением случаев, указанных в пункте 7 настоящего Порядка.

7. Нахождение в помещениях, в которых ведется обработка ИОД, посторонних лиц, возможно только в присутствии сотрудников Министерства, имеющих доступ к соответствующей информации.

8. Сотрудники Министерства, получившие доступ к ИОД, не должны покидать помещение, в котором ведется обработка ИОД, оставляя в нем без присмотра посторонних лиц, включая сотрудников, не уполномоченных на обработку такой информации. После окончания рабочего дня дверь каждого помещения закрывается на ключ. Дополнительно для защиты помещений могут применяться средства видеонаблюдения, охранной сигнализации и прочие средства защиты доступа.

9. В помещениях, в которых размещены и (или) хранятся носители ключевой, аутентифицирующей и парольной информации средств криптографической защиты информации (далее - МНИ СКЗИ), дополнительно должны применяться следующие меры, препятствующие возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в такие помещения:

утверждение правил доступа в помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

утверждения перечня лиц, имеющих право доступа в помещения.

10. Помещения, в которых размещены и (или) хранятся МНИ СКЗИ, предназначенные для защиты информации, содержащейся в ИС (сегмента ИС), предназначенной для решения задач ИС на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации, обрабатывающей информацию высокого уровня значимости, должны соответствовать следующим требованиям:

окна помещений, расположенных на первых и (или) последних этажах зданий, а также окна помещений, находящихся около пожарных лестниц и других мест, откуда возможно проникновение в помещения посторонних лиц, должны быть оборудованы металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения;

окна и двери помещений, в которых размещены серверы ИС, должны быть оборудованы металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения.

11. Ответственными за организацию доступа в помещения, в которых ведется обработка ИОД, являются руководители структурных подразделений Министерства.

12. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка ИОД, проводится должностным лицом, ответственным за соблюдение организационно-технических и режимных мер по защите информации в структурных подразделениях Министерства.

Приложение N 14
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

Типовая форма
акта об уничтожении персональных данных

Акт N _____
об уничтожении персональных данных

Комиссия в составе:
Председатель: ФИО, должность
Члены комиссии:
1. ФИО, должность
2. ФИО, должность
составила настоящий акт о том, что "___" _____ 202__ г. произведено уничтожение персональных данных (ПДн) субъекта ПДн _____ (категории уничтоженных ПДн: _____), оператором которых является Министерство государственного управления, информационных технологий и связи Московской области (юридический адрес: Московская область, г. Красногорск, бульвар Строителей, д. 1), обрабатываемых в информационных системах Министерства государственного управления, информационных технологий и связи Московской области: _____
Причина уничтожения ПДн: _____.
При уничтожении ПДн материальные носители не уничтожались/были уничтожены следующие материальные носители: _____.
Уничтожение ПДн было произведено посредством: _____.

Председатель комиссии:
Должность
_____ И.О. Фамилия

Члены комиссии:
Должность
_____ И.О. Фамилия
Должность
_____ И.О. Фамилия

Типовая форма
акта об уничтожении информации ограниченного доступа

Акт
об уничтожении информации ограниченного доступа

Комиссия в составе:
Председатель: ФИО, должность
Члены комиссии:
1. ФИО, должность
2. ФИО, должность
составила настоящий акт о том, что "___" _____ 2020 г. произведено уничтожение информации ограниченного доступа, а именно:
_____,
(описание уничтоженной информации)
с _____.
(заводской или учетный номер носителя информации)
Причина уничтожения информации ограниченного доступа с носителей информации
_____.
Уничтожение произведено посредством:
_____.

Председатель комиссии:
Должность
_____ И.О. Фамилия

Члены комиссии:
Должность
_____ И.О. Фамилия
Должность
_____ И.О. Фамилия

Приложение N 15
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ВОЗНИКНОВЕНИИ ВНЕШТАТНЫХ СИТУАЦИЙ

1. Назначение и область действия

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн в Министерстве государственного управления, информационных технологий и связи Московской области (далее - Министерство), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

Задачей данной Инструкции является:

определение мер защиты от прерывания;

определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех сотрудников Министерства, имеющих доступ к ресурсам ИСПДн.

2. Порядок реагирования на аварийную ситуацию

2.1. Действия при возникновении аварийной ситуации

В настоящем документе под аварийной ситуацией понимается некоторое происшествие,

связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники Министерства (либо подведомственных ему организаций) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с руководителями структурных подразделений. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

2.2. Уровни реагирования на инцидент

При реагировании на инцидент важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

Уровень 1 - незначительный инцидент. Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

Уровень 2 - авария. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

Уровень 3 - катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к прерыванию работоспособности ИСПДн и средств защиты на сутки и более.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций

3.1. Технические меры

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

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 Министерства (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.2. Организационные меры

Ответственные за реагирование сотрудники ознакомляют всех сотрудников Министерства, находящихся в их зоне ответственности, с данной инструкцией в срок, не превышающий 3 рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение должностных лиц Министерства, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Администраторы ИСПДн и администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.

> КонсультантПлюс: примечание.
> Нумерация разделов дана в соответствии с официальным текстом документа.

5. Действия в случае возникновения ситуаций, которые могут повлечь неправомерную передачу (предоставление, распространение, доступ) персональных данных

5.1. Уполномоченные должностные лица Министерства обязаны в порядке, определенном ФСБ России, обеспечивать взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн.

Взаимодействие Министерства с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование его о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) ПДн, осуществляется через Национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ) в соответствии с подпунктом 4.8 пункта 4 Положения о НКЦКИ.

5.2. Подтверждением передачи Министерством в НКЦКИ информации, указанной в п. 5.1 настоящей Инструкции, является присвоение НКЦКИ соответствующим компьютерным инцидентам идентификаторов. Идентификаторы направляются НКЦКИ в Министерство по тем же каналам, по которым Министерством была направлена информация о соответствующем инциденте в НКЦКИ.

5.3. В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) ПДн, повлекшей нарушение прав субъектов ПДн, Министерство обязано с момента выявления такого инцидента уведомить Роскомнадзор:

в течение двадцати четырех часов - о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов ПДн, и предполагаемом вреде, нанесенном правам субъектов ПДн, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения об уполномоченном должностном лице Министерства на взаимодействие с Роскомнадзором, по вопросам, связанным с выявленным инцидентом;

в течение семидесяти двух часов - о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Приложение N 16
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ТИПОВАЯ ФОРМА
ЖУРНАЛА УЧЕТА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЖУРНАЛ
учета событий информационной безопасности

Журнал начат "__" _____ 20__ г.	Журнал завершен "__" _____ 20__ г.
Должность	Должность
_____/_____/	_____/_____/

N п/п	Дата события	Основания возникновения события	Описание события (мероприятия)	Характеристика события	ФИО, субъекта	Должность, ФИО и подпись ответственного за ведение журнала	Примечание

Приложение N 17
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ТИПОВАЯ ФОРМА
ОБЯЗАТЕЛЬСТВА О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ
ОГРАНИЧЕННОГО ДОСТУПА

ОБЯЗАТЕЛЬСТВО
о неразглашении информации ограниченного доступа

Я, _____,
(фамилия, имя, отчество)
в качестве сотрудника Министерства государственного управления,
информационных технологий и связи Московской области (именуемого в
дальнейшем "Министерство") в период трудовых (служебных) отношений с
Министерством (ее правопреемником) и в течение лет после их окончания, в
соответствии с п. _____ трудового договора, заключенного между мной
и Министерством, а также соответствующими положениями по обеспечению защиты
и охраны информации ограниченного доступа, действующими в Министерстве,
обязуюсь:

не разглашать информацию ограниченного доступа Министерства, которая мне будут доверена или станет известна по работе (службе);

не передавать третьим лицам и не раскрывать публично информацию
ограниченного доступа Министерства без его согласия;

выполнять относящиеся ко мне требования приказов, инструкций и
положений по обеспечению сохранности информации ограниченного доступа
Министерства;

в случае попытки посторонних лиц получить от меня информацию ограниченного доступа Министерства немедленно сообщить руководителям структурных подразделений;

сохранять информацию ограниченного доступа тех организаций, с которыми у Министерства имеются деловые отношения;

не использовать знание информации ограниченного доступа Министерства для занятий любой деятельностью, которая может нанести ущерб Министерству;

в случае моего увольнения все носители информации ограниченного доступа Министерства (рукописи, черновики, чертежи, магнитные ленты, диски, дискеты, распечатки на принтерах, кино-, фотонегативы и позитивы, модели, материалы, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Министерстве, передать руководителю структурного подразделения;

об утрате или недостаче носителей информации ограниченного доступа, удостоверений, пропусков, ключей от режимных помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению конфиденциальной информации Министерства, а также о причинах и условиях возможной утечки сведений немедленно сообщать руководителю структурного подразделения.

Я предупрежден, что в случае невыполнения любого из пунктов настоящего обязательства могу быть уволен из Министерства. До моего сведения также доведены с разъяснениями соответствующие положения по обеспечению сохранности информации ограниченного доступа Министерства.

Мне известно, что нарушение этих положений может повлечь ответственность, предусмотренную законодательством Российской Федерации.

С перечнем документированной информации ограниченного доступа Министерства ознакомлен.

_____ _____
(подпись) (расшифровка подписи)
"__" _____ 20__ г.

Руководство Министерства подтверждает, что данные Вами обязательства не ограничивают Ваших прав на интеллектуальную собственность. Об окончании срока действия обязательства руководство Министерства уведомит Вас заблаговременно в письменной форме.

_____ _____
(подпись) (расшифровка подписи)
"__" _____ 20__ г.

Обязательства составлены в двух экземплярах. Один экземпляр находится у сотрудника, второй хранится в Министерстве в качестве приложения к трудовому договору или личному делу сотрудника.

Один экземпляр обязательств получил.

_____ _____
(подпись) (расшифровка подписи)
"__" _____ 20__ г.
(подпись) (расшифровка подписи)

Приложение N 18
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ТИПОВАЯ ФОРМА
ЖУРНАЛА УЧЕТА МАШИННЫХ НОСИТЕЛЕЙ ПЕРСОНАЛЬНЫХ ДАННЫХ
И ИНОЙ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Журнал
учета машинных носителей персональных данных
и иной информации ограниченного доступа

Журнал начат "__" _____ 20__ г.	Журнал завершен "__" _____ 20__ г.
Должность	Должность
_____/_____/	_____/_____/

N п/п	Вид материального носителя	Учетный номер	Дата постановки на учет	Ответственное лицо	Подпись ответственного лица	Дата выдачи	Номер акт уничтоже
1							
2							
3							
4							
5							
6							
7							
8							
9							

Приложение N 19
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 1 марта 2023 г. N 11-27/РВ

ТИПОВАЯ ФОРМА
АКТА РАССЛЕДОВАНИЯ ИНЦИДЕНТА

Акт
расследования инцидента

1. Состав комиссии расследования инцидента:
Председатель:
(должность, фамилия, инициалы)
Члены комиссии:
(должность, фамилия, инициалы)
2. Характеристика организации.

_____
Указать, были ли ранее аналогичные инциденты, отразить, как соблюдались требования по информационной безопасности.
3. Квалификация обслуживающего персонала, руководителей и специалистов объекта, ответственных лиц, причастных к инциденту.

_____
4. Обстоятельства инцидента, допущенные нарушения требований
законодательства.

_____
Описываются обстоятельства инцидента и сценарий его развития, указывается, какие факторы привели к инциденту и его последствиям (нарушение
законодательства, правил и др.).
5. Мероприятия по локализации и устранению причин инцидента.

_____
Излагаются меры по ликвидации последствий инцидента и предупреждению
подобных инцидентов, сроки выполнения мероприятий по устранению причин инцидента.
6. Заключение о лицах, ответственных за инцидент.

_____
Указываются лица, допустившие нарушения норм и правил безопасности, которые привели к инциденту. При этом указывается, какие требования нормативных документов не выполнены или нарушены конкретным лицом, исполнителем работ.
7. Ущерб от инцидента.

_____

Председатель:
(фамилия, инициалы, дата)

Члены комиссии:
(фамилия, инициалы, дата)