Распоряжение Мингосуправления МО 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"
(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 8 апреля 2021 г. 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

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 и ФСТЭК России, 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) Дроздова Максима Владимировича - первого заместителя министра государственного управления, информационных технологий и связи Московской области.

2. Назначить ответственным должностным лицом за защиту информации в Министерстве Коношенко Сергея Александровича - 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 Науменко Сергея Александровича - заведующего отделом информационной безопасности Управления специальных систем и информационной безопасности.

4. Назначить ответственным должностным лицом за рассмотрение запросов и обращений

субъектов персональных данных (представителей субъектов персональных данных), поступивших в Министерство, Мозгового Андрея Валериевича - главного инспектора отдела информационной безопасности Управления специальных систем и 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:

приказ Министерства государственного управления, информационных технологий и связи Московской области от 18.11.2015 N 10-95/П "Об организации работ по защите персональных данных при их обработке в информационных системах Министерства государственного управления, информационных технологий и связи Московской области";

приказ Министерства государственного управления, информационных технологий и связи Московской области от 04.07.2019 N 11-66/П "О внесении изменений в приказ Министерства государственного управления, информационных технологий и связи Московской области от 18.11.2015 N 10-95/П "Об организации работ по защите персональных данных при их обработке в информационных системах Министерства государственного управления, информационных технологий и связи Московской области".

7. Контроль за исполнением настоящего распоряжения оставляют собой.

Министр государственного управления,
информационных технологий и связи
Московской области
М.А. Рымар

Приложение N 1
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/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	Федеральный закон от 01.04.1996 N

	индивидуальных лицевых счетах	27-ФЗ "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования" (статья 6)
9.	Сведения о страхователе, застрахованном лице и выгодоприобретателе, состоянии их здоровья, а также об имущественном положении этих лиц	Гражданский кодекс Российской Федерации (статья 946)
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	Федеральный закон от 18.07.1999 N 183-ФЗ "Об экспортном контроле"

	должностных лиц органа государственного контроля при проведении проверок российских участников внешнеэкономической деятельности	(статья 17)
14.	Сведения, касающихся предмета договора на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода его исполнения и полученных результатов (в объеме, определенном договором)	Гражданский кодекс Российской Федерации (статья 771)
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,	Уголовный кодекс Российской

	применяемых в отношении должностного лица правоохранительного или контролирующего органа, а также его близких	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	Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне" (статья 3)

	введен режим коммерческой тайны	
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 8 апреля 2021 г. N 11-31/РВ

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

1. Общие положении

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", 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 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 информационных технологий и технических средств, обеспечивающих их обработку;

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

уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители 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 ПДн и иной 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. Действие настоящего Положения распространяется на все процессы обработки ИОД в Министерстве, включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн, осуществляемые с использованием средств автоматизации и без их использования.

1.5. 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.

1.6. Все изменения в Положение вносятся распоряжением Министерства.

1.7. 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 ограничиваться 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.

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. Обработка ПДн сотрудников Министерства может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия сотрудникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Министерства.

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 персональных данных, сокращение времени на их обработку;

контроль использования персональных данных; защита персональных данных;

воспрепятствование неправомерному доступу к персональным данным;

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

обмен персональными данными 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.

3.2. Персональные данные, обрабатываемые в Министерстве.

3.2.1. В Министерстве обрабатываются ПДн следующих субъектов ПДн:

сотрудников Министерства;

лиц, связанных с сотрудниками (родственники и т.д.);

потребителей услуг, оказываемых Министерством;

лиц, проживающих в Московской области;

клиентов организаций, контрагентов Министерства.

Данный перечень может пересматриваться по мере необходимости.

3.2.2. Персональные данные субъектов ПДн могут включать:

специальные категории ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

биометрические ПДн, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность;

общедоступные ПДн, которые получены только из общедоступных источников ПДН;

иные категории ПДн.

3.2.3. Полные списки обрабатываемых ПДн формируются в перечне ПДн, подлежащих защите, в ИСПДп Министерства.

4. Доступ к ИОД

4.1. Сотрудники Министерства, которые в силу выполняемых служебных обязанностей постоянно работают с ИОД, получают допуск к необходимым категориям ИОД на срок выполнения ими соответствующих должностных обязанностей в соответствии с утвержденными министром перечнями лиц, допущенных к работе с ИОД и с ПДн.

4.2. Списки лиц (должностей), имеющих доступ к ИОД для информационных систем, 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 на основании решения министра.

4.4. В целях реализации возложенных на Министерство задач, исполнение государственных функций и полномочий Министерства отдельные функции обработки ИОД, в том числе ПДн, 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.

4.6. 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. Предоставление информации по запросу или требованию органа государственной власти осуществляется с ведома министра.

4.7. В случае если сотруднику сторонней организации требуется доступ к ИОД Министерства, необходимо, чтобы в договоре со сторонней организацией были прописаны условия конфиденциальности ИОД и обязанность сторонней организации и ее сотрудников по соблюдению требований действующего законодательства Российской Федерации в области обработки и защиты ИОД, а также обработки и защиты ПДн. Кроме того, в случае доступа к ИОД, содержащей ПДн, лиц, не являющихся сотрудниками Министерства, должно быть получено согласие субъектов ПДн на предоставление их ПДн третьим лицам, если иное не определено законодательством Российской Федерации. Указанное согласие не требуется, если ПДн предоставляются в целях исполнения гражданско-правового договора, заключенного Министерством с субъектом ПДн.

4.8. 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 и к ПДн. В случае увольнения все находившиеся в распоряжении сотрудника в соответствии с его должностными обязанностями носители, содержащие ИОД, передаются руководителям структурных подразделений.

5. Основные требовании по защите ИОД

5.1. При обработке ИОД в информационных системах Министерства обеспечивается:

проведение мероприятий, направленных на предотвращение несанкционированного доступа к ИОД и (или) передачи ее лицам, не имеющим права доступа к такой информации;

своевременное обнаружение фактов несанкционированного доступа к ИОД;

недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

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

постоянный контроль обеспечения требований к защищенности ИОД и требуемого уровня защищенности ПДн.

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

5.3. На основании нормативно-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 ПДн при их обработке в ИСПДн (для каждой ИСПДн). Модели угроз безопасности ПДн для ИСПДн Министерства, имеющих статус государственных информационных систем (далее - ГИС), подлежат согласованию с ФСТЭК России и ФСБ России в пределах их полномочий.

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.

5.5. 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.

5.6. 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 и ПДн.

5.7. 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 подписать обязательство о неразглашении конфиденциальной информации (приложение N 17 к настоящему распоряжению).

5.8. 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.

5.9. 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.

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

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

6. Особенности обработки ИОД, содержащей ПДн, в Министерстве

6.1. Согласие на обработку ПДн.

6.1.1. 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, информированным и сознательным. 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.

6.1.2. 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.

6.2. Права субъекта в отношении ПДн, обрабатываемых Министерством.

6.2.1. 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 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. Перечень сведений и порядок получения сведений предусмотрен действующим 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;

давать предварительное письменное согласие при обработке ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации;

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.

6.3. Права и обязанности Министерства при обработке ПДн.

6.3.1. Министерство вправе:

6.3.1.1. 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 государственным или муниципальным органом соответствующего акта.

6.3.1.2. В случае отзыва субъектом ПДн согласия на обработку ПДн, продолжить обработку ПДн без согласия субъекта ПДн при наличии оснований, предусмотренных законодательством Российской Федерации.

6.3.1.3. 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.

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

6.3.4. Самостоятельно определять состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей Министерства, предусмотренных законодательством Российской Федерации.

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

6.3.2. Министерство обязано:

6.3.2.1. До начала обработки ПДн уведомить уполномоченный орган по защите прав субъектов ПДн о своем намерении осуществлять обработку ПДн, за исключением случаев, предусмотренных законодательством Российской Федерации.

6.3.2.2. При сборе ПДн, в том числе посредством информационно-телекоммуникационной сети Интернет, Министерство обеспечивает 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.

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

6.3.2.4. Представить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия законных оснований обработки ПДн без согласия субъекта ПДн.

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

6.3.2.6. Прекратить по требованию субъекта ПДн обработку его ПДн в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации.

6.3.2.7. 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.

6.3.2.8. При сборе ПДн предоставить субъекту ПДн по его просьбе информацию, предусмотренную законодательством Российской Федерации.

Если предоставление ПДн Министерству для субъекта ПДн является обязательным в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", оно обязано разъяснить субъекту ПДн юридические последствия его отказа предоставить ПДн.

6.3.2.9. Если ПДн получены не от субъекта ПДн, Министерство, за исключением случаев, предусмотренных законодательством Российской Федерации, до начала обработки таких ПДн должно предоставить субъекту ПДн следующую информацию:

наименование и адрес Министерства либо фамилия, имя, отчество его представителя;

цель обработки ПДн и ее правовое основание;

предполагаемые пользователи ПДн;

установленные права субъекта персональных данных;

источник получении ПДн.

6.3.2.10. Принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей Министерства, предусмотренных законодательством Российской Федерации.

6.3.2.11. Опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки ПДн, к сведениям о реализуемых требованиях по защите ПДн.

При осуществлении сбора ПДн с использованием информационно-телекоммуникационных

сетей опубликовать в соответствующей информационно-телекоммуникационной сети документ, определяющий его политику в отношении обработки ПДн, и сведения о реализуемых требованиях по защите ПДн, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети.

6.3.2.12. 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.

6.3.2.13. 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.

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

6.3.2.15. Назначить должностное лицо, ответственное за организацию обработки ПДн.

7. Порядок обработки и защиты ИОД

7.1. Обеспечение конфиденциальности ИОД, обрабатывающейся Министерством, является обязательным требованием для всех лиц, которым ИОД стала известна.

7.2. Сотрудники Министерства, осуществляющие оформление документов, содержащих ПДн, обязаны получать согласие субъектов ПДн на обработку, за исключением случаев, предусмотренных законодательством Российской Федерации.

7.3. В случае нарушения установленного порядка обработки ИОД сотрудники Министерства несут ответственность в соответствии с разделом 9 настоящего Положения.

7.4. ИОД на бумажных носителях, обрабатываемая Министерством, 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 носителей ИОД осуществляется их восстановление (по возможности).

7.5. 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 от 20 января 2016 г. N 11-ПГ "Об утверждении Правил делопроизводства в исполнительных органах государственной власти Московской области, государственных органах 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).

7.6. Выдача документов для ознакомления осуществляется лицам, допущенным к соответствующей информации в целях исполнения должностных обязанностей, на срок не более одного рабочего дня.

7.7. При работе с программными средствами информационной системы Министерства, реализующей функции просмотра и редактирования ИОД, запрещается демонстрация экранных форм, содержащих такие данные, лицам, не имеющим соответствующего допуска.

7.8. При получении ИОД сотрудником Министерства, который в соответствии с должностными обязанностями получает ПДн от клиента, сотрудника, иного лица, в обязательном порядке проводится проверка достоверности ИОД. Ввод ИОД, полученной Министерством, в информационную систему, осуществляется сотрудниками, имеющими доступ к соответствующей информации. Сотрудники, осуществляющие ввод информации, несут ответственность за достоверность и полноту введенной информации.

7.9. Особенности обработки ИОД, содержащей ПДн, на бумажных носителях, без использования средств автоматизации (в случаях, если при обработке ПДн не используется ПЭВМ) установлены постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

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

7.9.2. При неавтоматизированной обработке ПДн на бумажных носителях:

7.9.2.1. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых несовместимы между собой.

7.9.2.2. ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

7.9.3. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них ПДн (далее - типовые формы), должны соблюдаться следующие условия:

7.9.3.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес Министерства, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых способов обработки ПДн.

7.9.3.2. Типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, при необходимости получения письменного согласия на обработку ПДн.

7.9.3.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, не нарушая прав и законных интересов иных субъектов ПДн.

7.9.3.4. Типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых различны.

7.10. Хранение ИОД, содержащей 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, выгодоприобретателем или поручителем по которому является субъект ПДн.

7.11. Порядок уничтожения, блокирования и уточнения ИОД.

7.11.1. Уничтожение ИОД, в том числе обезличивание части ПДн, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этой информации с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

7.11.2. Уточнение ИОД, в том числе ПДн, 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.

7.12. Уничтожение носителей, содержащих ИОД, осуществляется в следующем порядке:

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

7.12.2. ИОД, размещенная в памяти ПЭВМ, удаляется с использованием программного обеспечения гарантированного удаления данных в установленном законодательством Российской Федерации порядке.

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

7.13. Об уничтожении носителя информации составляется акт об уничтожении ИОД (акт об уничтожении ПДн) (приложение N 14 к настоящему распоряжению).

7.14. По окончании рабочего дня сотрудники Министерства закрывают в служебных помещениях окна, запирают данные помещения и включают сигнализацию (при наличии).

7.15. Сетевое оборудование, серверы следует располагать в местах, недоступных для посторонних лиц (в специальных помещениях, шкафах, коробах).

7.16. Уборка помещений и обслуживание технических средств ИС должны осуществляться

под контролем ответственных за данные помещения и технические средства лиц с соблюдением мер, исключающих несанкционированный доступ к ИОД, носителям информации, программным и техническим средствам обработки, передачи и защиты информации ИС.

7.17. В обязанности администраторов ИС входит управление учетными записями пользователей, поддержание штатной работы ИС, обеспечение резервного копирования данных, а также установка и конфигурирование аппаратного и программного обеспечения ИС, не связанного с обеспечением безопасности ИОД. Кроме того, в их обязанности входит обеспечение соответствия порядка обработки и безопасности ИОД в ИС требованиям по конфиденциальности, целостности и доступности ИОД, предъявляемым к конкретной ИС, и общим требованиям по безопасности ИОД, установленным законодательством Российской Федерации.

7.18. В обязанности администраторов ИС входит установка, конфигурирование и администрирование аппаратных и программных средств защиты информации ИС, учет и хранение машинных носителей ИОД, периодический аудит журналов безопасности и анализ защищенности ИС, а также участие в служебных расследованиях фактов нарушения установленного порядка обработки и обеспечения безопасности ИОД.

7.19. В целях обеспечения распределения полномочий, реализации взаимного контроля и недопущения сосредоточения представляющих угрозу для безопасности ИОД полномочий у одного лица не рекомендуется назначать администраторами ИС их пользователей.

7.20. Квалификационные требования и детальный перечень прав и обязанностей администраторов ИС закрепляются в соответствующих должностных инструкциях, ознакомление с которыми подтверждается подписью назначаемых сотрудников.

7.21. Организация внутреннего контроля процесса обработки ИОД в Министерстве осуществляется 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.

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

7.22.1. Обеспечение соблюдения сотрудниками Министерства требований настоящего Положения и нормативных правовых актов, регулирующих процессы обработки и защиты ИОД, обработки и защиты ПДн.

7.22.2. Оценка компетентности персонала, задействованного в обработке ИОД.

7.22.3. Обеспечение работоспособности и эффективности технических средств ИС и средств защиты ИОД, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности ИОД.

7.22.4. Выявление нарушений установленного порядка обработки ИОД и своевременное предотвращение негативных последствий таких нарушений.

7.22.5. Принятие корректирующих мер, направленных на устранение выявленных нарушений

в процессе обработки ИОД и в работе технических средств ИС.

7.22.6. Разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности ИОД по результатам контрольных мероприятий.

7.22.7. Осуществление внутреннего контроля исполнения рекомендаций и указаний по устранению нарушений.

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

7.22. 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.

8. Передача (предоставление) ИОД

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

действующего законодательства Российской Федерации;

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

для ИОД, содержащей ПДн, - письменного согласия субъекта ПДн на передачу его ПДн третьей стороне, за исключением случаев, предусмотренных законодательством Российской Федерации.

8.2. Особенности передачи (предоставления) ИОД, содержащей ПДн.

8.2.1. Трансграничная передача ИОД, содержащей ПДн, на территорию иностранных государств может осуществляться Министерством в соответствии с положениями ст. 12 Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных". Трансграничная передача ПДн на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн, может осуществляться при наличии согласия в письменной форме субъекта ПДн на трансграничную передачу его ПДн, либо в случаях:

предусмотренных международными договорами Российской Федерации;

предусмотренных законодательством Российской Федерации, если это необходимо в целях защиты основ конституционного строя Российской Федерации, обеспечения обороны страны и безопасности государства, а также обеспечения безопасности устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

исполнения договора, стороной которого является субъект ПДн;

защиты жизни, здоровья, иных жизненно важных интересов субъекта ПДн или других лиц при невозможности получения согласия в письменной форме субъекта ПДн.

8.2.2. 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.

8.2.3. 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 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 ИОД;

утраты материальных носителей ИОД;

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

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

Приложение N 3
к распоряжению Министерства
государственного управления,
информационных технологий и связи

Московской области
от 8 апреля 2021 г. N 11-31/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 N 149-ФЗ от 27 июля 2006 г. "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", Правилами делопроизводства в исполнительных органах государственной власти Московской области, государственных органах Московской области, утвержденными постановлением Губернатора Московской области от 20 января 2016 г. N 11-ПГ "Об утверждении Правил делопроизводства в исполнительных органах государственной власти Московской области, государственных органах Московской области", и устанавливает порядок учета и использования машинных носителей информации для обработки персональных данных (далее - ПДн).

Действие настоящего Положения об учете съемных носителей ПДн и иной информации ограниченного доступа распространяется на всех сотрудников Министерства, подрядчиков и представителей третьей стороны.

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.

ИСПДн - информационная система персональных данных.

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

ПК - персональный компьютер.

ПО - программное обеспечение вычислительной техники.

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

Пользователь - сотрудник Министерства, использующий ПК и носители информации для выполнения своих служебных обязанностей.

3. Порядок использования машинных носителей информации

3.1. Под использованием МНИ в ИС понимается их подключение к инфраструктуре ИС с целью обработки ПДн (иной информации ограниченного доступа, далее - ИОД) и обмена информацией между ИСПДн (ИС) и МНИ.

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

3.3. К МНИ ПДн (ИОД) предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется администраторами ИС).

3.4. МНИ ПДн (ИОД) предоставляются по инициативе руководителей структурных подразделений Министерства в случаях:

необходимости выполнения новым пользователем своих должностных обязанностей;

возникновения у пользователя производственной необходимости.

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

4.1. Все находящиеся на хранении и в обращении съемные МНИ ПДн (ИОД) подлежат учету.

4.2. Каждый съемный МНИ ПДн (ИОД) должен иметь уникальный учетный номер.

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

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

4.5. При использовании пользователями МНИ ПДн необходимо:

соблюдать требования настоящего Положения;

использовать МНИ ПДн (ИОД) исключительно для выполнения своих служебных обязанностей;

ставить в известность администраторов ИС о любых фактах нарушения требований

настоящего Положения;

бережно относится к МНИ ПДн (ИОД);

обеспечивать безопасность МНИ ПДн (ИОД) всеми возможными способами;

извещать администраторов ИС о фактах утраты (кражи) МНИ ПДн (ИОД).

4.6. При использовании МНИ ПДн (ИОД) запрещается:

использовать их в личных целях;

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

хранить их вместе с общедоступными данными на рабочих столах либо оставлять без присмотра или передавать на хранение другим лицам; выносить их из служебных помещений для работы на дому.

4.7. Обработка, прием и передача ПДн (ИОД), инициированное сотрудником между ИС и неучтенными МНИ, рассматривается как несанкционированное. Администратор ИС оставляет за собой право блокировать или ограничивать использование МНИ ПДн (ИОД).

4.8. В случае выявления фактов несанкционированного и (или) нецелевого использования МНИ ПДн (ИОД) инициируется служебная проверка, проводимая комиссией, состав и полномочия которой определяется приказом Министерства. 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 действующим законодательством Российской Федерации.

4.9. Информация, хранящаяся на МНИ ПДн (ИОД), подлежит обязательной проверке на предмет отсутствия вредоносного ПО.

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

4.11. Вынос съемных МНИ ПДн (ИОД) для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

4.12. В случае утраты или несанкционированного уничтожения съемных МНИ ПДн (ИОД) 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 съемных носителей ПДн (ИОД) вносятся соответствующие отметки.

4.13. Съемные МНИ ПДн (ИОД), пришедшие в негодность, или отслужившие установленный

срок, подлежат уничтожению.

4.14. В случае увольнения или перевода сотрудника в другое структурное подразделение предоставленные ему МНИ ПДн (ИОД) 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 ПДн (ИОД) с составлением соответствующего акта об уничтожении;

удалить информацию, содержащуюся на МНИ ПДн (ИОД), с помощью специального программного обеспечения, сертифицированного ФСТЭК России, с составлением соответствующего акта об уничтожении (очистке);

сдать в архив или перерегистрировать МНИ ПДн (ИОД) на структурное подразделение и сделать соответствующую отметку в Журнале.

5. Ответственность

Пользователи и администраторы информационной системы, нарушившие требования настоящего Положения, несут ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение N 4
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/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) определяются порядок учета (регистрации), рассмотрения запросов субъектов ПДн или их представителей (далее - 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", от 27 июля 2004 г. N 79-ФЗ "О государственной гражданской службе Российской Федерации", Трудовым кодексом Российской Федерации от 30 декабря 2001 г. N 197-ФЗ, 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".

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 в Министерстве сведений 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 Федеральным законом;

сроки обработки и хранения ПДн;

порядок осуществления субъектом ПДн прав, предусмотренных Федеральным законом;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

иные сведения, предусмотренные Федеральным законом.

3.2. Право субъекта ПДн на доступ к его ПДн может быть ограничено в соответствии со статьей 14 Федерального закона.

3.3. 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.

Сведения, указанные в пункте 3.1 Правил должны быть предоставлены субъекту ПДн 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.

3.4. Сведения, указанные в пункте 3.1 Правил предоставляются субъекту ПДн или его представителю при обращении либо при получении запроса субъекта ПДн или его представителя.

3.5. 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 (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), 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 электронной подписью в соответствии с законодательством Российской Федерации.

3.6. 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.

3.7. 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.

3.8. Запрос рассматривается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. В случае если сведения, указанные в пункте 3.1 Правил, были предоставлены для ознакомления субъекту ПДн по его запросу ранее, субъект ПДн вправе обратиться повторно в Министерство или направить повторный запрос в целях получения сведений, указанных в пункте 3.1 Правил, и ознакомления с такими ПДн 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 ПДн.

Субъект ПДн вправе обратиться повторно в Министерство или направить повторный запрос в целях получения сведений, указанных в пункте 3.1 Правил, а также в целях ознакомления с обрабатываемыми ПДн до истечения срока, указанного в настоящем пункте, в случае если такие сведения и (или) обрабатываемые ПДн не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

3.9. Министерство вправе отказать субъекту ПДн в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона. Такой отказ должен быть мотивированным.

3.10. 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 тридцати дней с даты получения запроса субъекта ПДн или его представителя.

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 субъекта ПДн или его представителя уполномоченные должностные лица Министерства обязаны дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий тридцати дней со дня регистрации обращения субъекта ПДн или его представителя либо с даты получения запроса субъекта ПДн или его представителя.

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

3.13. 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.

3.14. 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).

3.15. 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.

3.16. 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.

3.17. 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.

3.18. 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.

3.19. 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.

3.20. Рассмотрение запросов 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 запросов могут привлекаться представители организаций, подведомственных Министерству, при условии соблюдения требований законодательства Российской Федерации.

3.21. 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 Федеральным законом или другими федеральными законами.

4.2. В случае отсутствия возможности уничтожения ПДн в течение срока, указанного в 4.1 Правил, 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 федеральными законами.

4.3. Отзыв согласия, данного Министерству, осуществляется посредством обращения либо направления запроса субъекта ПДн или его представителя в Министерство.

4.4. Отзыв согласия, данного организации, по поручению которой Министерство

осуществляет обработку ПДн, 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 отзыве согласия.

4.5. Регистрация запроса (обращения) субъекта ПДн либо письма с информацией о наличии запроса (обращения) от организации, по поручению которой Министерство обрабатывает ПДн, осуществляется в соответствии с правилами делопроизводства, действующими в Министерстве, после чего запрос (обращение, письмо) в установленном в Министерстве порядке направляется для дальнейшего рассмотрения лицу, за рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей.

4.6. Порядок действий в случае принятия решения о необходимости удаления ПДн субъекта ПДн на основании отзыва согласия.

4.6.1. В случае принятия решения о необходимости удаления ПДн субъекта ПДн они подлежат удалению сотрудниками Министерства, имеющими соответствующие полномочия по доступу к ИСПДн Министерства, после чего оформляется акт удаления ПДн в соответствии с формой (приложение N 14 к настоящему распоряжению). Акт удаления ПДн подписывается Комиссией в составе:

глава Комиссии - должностное лицо, ответственное за организацию обработки ПДн в Министерстве;

члены Комиссии - должностное лицо, ответственное за рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей, а также должностные лица, ответственные за функционирование ИСПДн, из которых осуществляется удаление ПДн в соответствии с отзывом согласия.

4.6.2. Акты удаления ПДн хранятся у должностного лица, ответственного за рассмотрение запросов и обращений в Министерство субъектов ПДн или их представителей.

4.6.3. Копия акта удаления 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.

4.6.4. Копия акта удаления ПДн, удаленных по результатам рассмотрения письма от организации, по поручению которой Министерство осуществляет обработку ПДн (либо от организации, в которую субъект ПДн или его представитель обращался по вопросам предоставления согласия Министерству на обработку его ПДн и 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.

4.6.5. 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).

4.6.6. Действие п. 4.6.5 Правил не распространяется на случаи передачи ПДн третьим лицам (организациям), не предусматривающие необходимость согласия субъекта ПДн на такую передачу.

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

4.7.1. 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 обрабатываемых Министерством ПДн, согласие на обработку которых отозвано;

невозможности однозначной идентификации субъекта ПДн или однозначного 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;

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

4.7.2. 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, по поручению которой Министерство обрабатывает ПДн. в ответ на соответствующее письмо, в порядке, установленном в Министерстве.

4.7.3. В случае если отзыв согласия был направлен в Министерство организацией, по поручению которой Министерство осуществляет обработку ПДн (либо организацией, в которую субъект ПДн или его представитель обращался по вопросам предоставления согласия Министерству на обработку его ПДн и 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.

4.8. 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 и т.п.).

4.9. 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 информационных систем, из которых требуется удалить

ПДн, удалению подлежат ПДн субъекта, обрабатываемые в указанных информационных системах (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.

4.10. ПДн, обработка которых Министерством в соответствии с Федеральным законом не требует наличия согласия субъекта ПДн, по результатам рассмотрения соответствующего отзыва согласия, удалению не подлежат.

4.11. ПДн, обработка которых в Министерстве началась после даты отзыва согласия, по результатам его рассмотрения удалению не подлежат.

4.12. Рассмотрение отзывов согласий, а также писем от организаций, по поручению которых Министерство обрабатывает ПДн, 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.

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

5. 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.

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

7. 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 8 апреля 2021 г. N 11-31/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 определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области обработки информации ограниченного доступа (далее - ИОД), в том числе персональных данных (далее - ПДн), 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, исполнение 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 обработке и защите ИОД, обработке и защите ПДн в ИС Министерства проводятся в следующих целях:

проверка выполнения требований организационно-распорядительной документации по защите информации в Министерстве и действующего законодательства Российской Федерации в

области обработки и защиты ИОД, обработки и защиты ПДн;

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

оценка обоснованности и эффективности применяемых мер и средств защиты ИОД.

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

2.1. Проверки соответствия обработки ИОД установленным требованиям в Министерстве разделяются на следующие виды:

регулярные;

плановые;

внеплановые.

2.2. Регулярные контрольные мероприятия периодически проводятся администратором ИС в соответствии с утвержденным планом проведения контрольных мероприятий (далее - План) и предназначены для осуществления контроля выполнения требований в области защиты ИОД в Министерстве.

2.3. Плановые контрольные мероприятия периодически проводятся Комиссией по обследованию режимных помещений, категорированию и классификации объектов информатизации и по оценке эффективности мер по обеспечению безопасности информации, включая персональные данные в информационных системах Министерства государственного управления, информационных технологий и связи Московской области в соответствии с утвержденным Планом 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 и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

по результатам расследования инцидента информационной безопасности;

по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

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

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий должностное лицо,

ответственное за выполнение работ по защите информации в Министерстве, разрабатывает план внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

цели проведения контрольных мероприятий;

задачи проведения контрольных мероприятий;

объекты контроля (процессы, подразделения, информационные системы и т.п.);

состав участников, привлекаемых для проведения контрольных мероприятий;

сроки и этапы проведения контрольных мероприятий.

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

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в журнале учета событий информационной безопасности (приложение N 16 к распоряжению).

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий ответственное лицо или члены комиссии разрабатывают отчет, в котором указывается:

описание проведенных мероприятий по каждому из этапов;

перечень и описание выявленных нарушений;

рекомендации по устранению выявленных нарушений;

заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Отчет передается на рассмотрение министру.

4.4. Общая информация о проведенном контрольном мероприятии фиксируется в журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки ИОД требованиям к защите информации в Министерстве.

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия в отношении ИС проводятся при обязательном участии лица, за выполнение работ по защите информации и контроль соблюдения организационно-технических и режимных мер по защите информации в структурных подразделениях Министерства, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы ИС и ответственные за обеспечение безопасности информации в ИС.

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

5.3. Должностное лицо, ответственное за защиту информации в Министерстве, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План. При проведении внеплановых контрольных мероприятий уведомление не требуется.

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

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

соответствия полномочий Пользователя правилам доступа;

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 и защиты ПДн;

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);

знания Пользователями положений инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций (приложение N 15 к настоящему распоряжению);

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

порядок и условия применения средств защиты информации; состояние учета машинных носителей 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 средств защиты;

технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

Приложение N 1
к приложению N 5 к распоряжению
Министерства государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/РВ

Типовая форма плана
внутренних проверок контроля соответствия
обработки информации ограниченного доступа требованиям
к защите информации

План
внутренних проверок контроля соответствия обработки
информации ограниченного доступа требованиям
к защите информации

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель

Приложение N 2
к приложению N 5 к распоряжению
Министерства государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/РВ

Типовая форма протокола
проведения внутренних проверок контроля соответствия
обработки информации ограниченного доступа требованиям
к защите информации

ПРОТОКОЛ N ____
проведения внутренних проверок контроля соответствия
обработки информации ограниченного доступа требованиям
к защите информации

Настоящий протокол составлен о том, что "___" _____ 20__ г.
_____ (комиссией)
(должность, Ф.И.О. сотрудника)
проведена проверка _____
(тема проверки)
Проверка осуществлялась в соответствии с требованиями:
_____
(название документа)
_____

В ходе проверки проверено:
_____
_____
_____
_____
_____

Выявленные нарушения:
_____
_____

_____
_____
_____

Меры по устранению нарушений:

_____
_____
_____
_____
_____
_____

Срок устранения нарушений: _____

Председатель комиссии:
фамилия и инициалы/подпись/должность

Члены комиссии:
фамилия и инициалы/подпись/должность
фамилия и инициалы/подпись/должность

Приложение N 6
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/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 невозможно определить принадлежность ПДн конкретному субъекту ПДн.

3. Условия обезличивания

Обезличивание ПДн может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых ПДн, снижения классов ИСПДн и по достижении 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 министр либо должностное лицо, ответственное за защиту информации в Министерстве;

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

сотрудники подразделений, обслуживающих базы данных с ПДн, совместно с должностным лицом, ответственным за организацию обработки ПДн, осуществляют непосредственное обезличивание выбранным способом.

4 Порядок работы с обезличенными ПДн

Обезличенные данные не подлежат разглашению и нарушению конфиденциальности, если иное не определено федеральными законами и принятыми во их основание нормативными

правовыми актами.

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

При обработке обезличенных данные необходимо соблюдение требований нормативных правовых актов Российской Федерации и Московской области.

Приложение N 7
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/РВ

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

Приложение N 8
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/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.	Начальник управления экономического планирования,	ПДн, обрабатываемые в связи с реализацией трудовых отношений, а

	правовой и кадровой работы и его заместители	также в связи с оказанием государственных услуг и осуществлением государственных функций; ПДн гражданских служащих и сотрудников структурных подразделений; ПДн граждан, обрабатываемые в целях оказания государственных услуг, контроля за оказанием государственных услуг, выполнения договорных обязательств Министерства, реализации возложенных на Министерство задач, исполнения государственных функций и полномочий Министерства
2.	Начальник отдела планирования, экономики и бухгалтерского учета	
3.	Начальник отдела кадровой работы	
4.	Сотрудники подразделений, участвующих в реализации функций и полномочий Министерства, предусматривающих необходимость обработки персональных данных, в том числе в процессах оказания государственных услуг и обработки обращений граждан	

Приложение N 9
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/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 организации (далее - Инструкция), 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 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 обязано:

осуществлять внутренний контроль 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, 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 о ПДн должностное лицо, ответственное за организацию обработки ПДн, несет предусмотренную законодательством Российской Федерации ответственность.

Приложение N 10
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области

от 8 апреля 2021 г. N 11-31/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 об обработке и защите персональных данных в Мингосуправления 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 8 апреля 2021 г. N 11-31/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.
_____/Ф.И.О. сотрудника/"___" _____ 20__ г.
(подпись) (дата подписи)

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

Согласие на обработку персональных данных

Я, _____
(Фамилия, имя, отчества 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 центральных исполнительных органов 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 центральных 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 совершения 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 подтверждаю 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 _____/____/

Приложение N 12
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/РВ

Типовая форма
разъяснения субъекту персональных данных
юридических последствий отказа предоставить свои
персональные данные

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 случае отказа Вами предоставить свои персональные данные, 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)

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 8 апреля 2021 г. N 11-31/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) 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 персональным данным субъектов персональных данных и к иной информации ограниченного доступа в Мингосуправления Московской области.

3. Персональные данные относятся к информации ограниченного доступа.

Сотрудники Мингосуправления Московской области, получившие доступ к персональным данным и иной информации ограниченного доступа, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", а также не распространять иную информацию ограниченного доступа, за исключением случаев, определенных законодательством Российской Федерации.

4. Обеспечение безопасности персональных данных (иной информации ограниченного доступа) от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные (информация ограниченного доступа) в информационной системе и без использования средств автоматизации.

5. Для помещений, в которых обрабатываются персональные данные (информация ограниченного доступа), организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных (информации ограниченного доступа) и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

При хранении материальных носителей персональных данных (информация ограниченного доступа) 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 персональных данных (информации ограниченного доступа), а также хранятся указанные носители информации, допускаются только сотрудники Мингосуправления Московской области и подведомственных Мингосуправления Московской области организаций, получившие доступ к персональным данным (информация ограниченного доступа), за исключением случаев, указанных в пункте 7 настоящего Порядка.

7. Нахождение в помещениях, в которых ведется обработка персональных лиц (информация ограниченного доступа), не являющихся сотрудниками, получившими доступ к указанной информации, возможно только в присутствии сотрудников, получивших доступ к ней на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных функций и (или) осуществлением полномочий в рамках договоров.

8. Сотрудники Мингосуправления Московской области, получившие доступ к персональным данным (информации ограниченного доступа), не должны покидать помещение, в котором ведется обработка персональных данных (информации ограниченного доступа), 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.

9. Ответственными за организацию доступа в помещения, в которых ведется обработка персональных данных (информации ограниченного доступа), являются руководители структурных подразделений Мингосуправления Московской области.

10. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных (информации ограниченного доступа), проводится должностным лицом, ответственным за организацию обработки персональных данных (в случае иной информации ограниченного доступа - 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 8 апреля 2021 г. N 11-31/РВ

Типовая форма
акта об уничтожении персональных данных
(информации ограниченного доступа)

Акт
об уничтожении персональных данных
(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 персональных данных (информации ограниченного доступа). обрабатываемых в (находящихся на)

_____
_____
_____
(наименование ИС по утвержденной конфигурации
(заводской или учетный номер носителя информации)

Причина удаления персональных данных (информации ограниченного доступа) из информационных систем (с носителей информации)

_____.

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 8 апреля 2021 г. N 11-31/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 Мингосуправления Московской области, 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 Мингосуправления Московской области, 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 Мингосуправления Московской области (либо подведомственных Мингосуправления Московской области 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.

К авариям относятся следующие инциденты:

Отказ элементов ИСПДн и средств защиты из-за:

повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей;

сбоя системы кондиционирования.

Отсутствие администратора ИСПДн и администратора безопасности более чем на сутки из-за:

химического выброса в атмосферу; сбоев общественного транспорта; эпидемии;

массового отравления персонала;

сильного снегопада;

торнадо;

сильных морозов.

Уровень 3 - Катастрофа. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, 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.

К катастрофам относятся следующие инциденты:

пожар в здании;

взрыв;

просадка грунта с частичным обрушением здания; массовые беспорядки в непосредственной близости.

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 Мингосуправления Московской области (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 Мингосуправления Московской области, 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 Мингосуправления Московской области, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

оказание первой медицинской помощи;

пожаротушение;

эвакуация людей;

защита материальных и информационных ресурсов;

методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;

выключение оборудования, электричества, водоснабжения, газоснабжения. 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.

Приложение N 16
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/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 8 апреля 2021 г. N 11-31/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.

Приложение N 18
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/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 акта об уничтожен ни

1							
2							
3							
4							
5							
6							
7							
8							
9							

Приложение N 19
к распоряжению Министерства
государственного управления,
информационных технологий и связи
Московской области
от 8 апреля 2021 г. N 11-31/РВ

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

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 последствия" (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 мероприятии по устранению причин инцидента

5. 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

6. Ущерб от инцидента.

Председатель: (фамилия, инициалы, дата)
Члены комиссии: (фамилия, инициалы, дата)