Приложение
к приказу ГБУК г. Москвы «ГМЗ «Царицыно»
от 28 июля 2021 г. № 378

# Положение
# о защите персональных данных

## 1. Общие положения

1.1. Настоящее Положение о защите персональных данных (далее – Положение) разработано ГБУК г. Москвы «ГМЗ «Царицыно» (далее – Оператор, Музей) в целях в целях сохранения личной тайны и защиты персональных данных.

1.2. Положение разработано на основе и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, федеральных законов от 27.07.2006 № 152-ФЗ «О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», положений главы 14 Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.3. Положение определяет права и обязанности руководителей и работников, порядок использования персональных данных в служебных целях, а также порядок взаимодействия по поводу сбора, документирования, хранения и уничтожения персональных данных.

1.4. В настоящем Положении используются следующие понятия и термины:

СКЗИ - средства криптографической защиты информации;

АРМ - автоматизированное рабочее место;

АИС - автоматизированная информационная система;

БД - база данных;

ОС - операционная система;

персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, паспортные данные или данные иного документа, удостоверяющего личность, дата и место рождения, адрес, регистрация, семейное, социальное, имущественное положение, образование, профессия, данные трудовой книжки, доходы, другая информация, однозначно позволяющая идентифицировать личность;

Оператор - юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных;

обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование,


ПРАВИТЕЛЬСТВО МОСКВЫ

распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

использование персональных данных - действия (операции) с персональными данными, совершаемые Оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

конфиденциальность персональных данных - обязательное для соблюдения Оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

1.5. Настоящее Положение устанавливает требования к защите и обеспечению безопасности ПДн при их автоматизированной и неавтоматизированной обработке в Музее, представляющих собой совокупность ПДн, содержащихся в базах данных Музея, а также данных на материальных носителях.

1.6. Под техническими средствами, позволяющими осуществлять обработку ПДн, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн, программные средства (операционные системы, системы управления базами данных и т.п.),


ПРАВИТЕЛЬСТВО МОСКВЫ

средства защиты информации, применяемые в информационных системах Музея.

Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты ПДн, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1.7. Целью настоящего Положения является обеспечение конфиденциальности и безопасности ПДн при их обработке:

исключение возможности несанкционированного доступа к ПДн и использования этих данных работниками Музея и третьими лицами в собственных интересах в ущерб интересам посетителей Музея и интересам самого Музея;

минимизация рисков предъявления претензий к Музею со стороны правоохранительных и иных государственных органов, а также юридических и физических лиц.

1.8. Сотрудниками Музея и третьими лицами, получающими доступ к ПДн, должна обеспечиваться конфиденциальность таких данных.

Обеспечение конфиденциальности ПДн не требуется:

в случае обезличивания ПДн;

в отношении общедоступных ПДн.

1.9. Общедоступные источники ПДн.

В целях информационного обеспечения могут создаваться общедоступные источники ПДн (в том числе справочники, адресные книги и т.д.). Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников ПДн по требованию субъекта ПДн, либо по решению суда или иных уполномоченных государственных органов.

## 2. Обязанности оператора по защите ПДн

2.1. Меры по защите и обеспечению безопасности ПДн при их обработке.



ПРАВИТЕЛЬСТВО МОСКВЫ

Оператор при обработке ПДн обязан принимать необходимые организационные и технические меры для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также от иных неправомерных действий.

В случае достижения цели обработки ПДн Оператор обязан незамедлительно прекратить обработку ПДн и уничтожить соответствующие ПДн.

2.2. Принимаемые меры для защиты ПДн.

2.2.1. Организационные:

размещение в разных помещениях сотрудников Музея, выполняющих различные виды профессиональной деятельности;

ограничение доступа посторонних лиц в помещения подразделений Музея, предназначенных для осуществления профессиональной деятельности;

размещение подразделений Музея и оборудования способом, исключающим возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц, включая работников других подразделений;

ограничение доступа посторонних лиц в помещения Музея после окончания рабочего дня;

ограничение доступа сотрудников и посторонних лиц в помещения Музея по выходным и праздничным дням;

контроль за доступом в помещение с установленным серверным оборудованием;

АИС;

модель угроз безопасности ПДн при их обработке в ИСПДн Музея.

2.2.2. Физические:

физическая защита здания Музея и в т.ч. защита помещений;

пропускная система при входе в служебные помещения Музея;

размещение АРМ в контролируемых помещениях и разграничение доступа сотрудников к ним;

размещение серверного и сетевого оборудования в отдельном, контролируемом и запирающемся помещении;

наличие несгораемых сейфов для хранения ключевых носителей и документов;

использование жалюзи (штор) для защиты окон помещений, находящихся на первом этаже служебных помещений Музея, для предотвращения просмотра информации, выведенной на экраны мониторов;

расположение мониторов ПЭВМ, обрабатывающих ПДн, порядком, препятствующим визуальному считыванию посторонними лицами информации с экранов мониторов.

2.2.3. Технические:



ПРАВИТЕЛЬСТВО МОСКВЫ

система контроля управления доступом;

пожарно-охранная сигнализация;

наличие запирающих устройств (замков) на дверях помещений и кабинетах;

наличие у всех дверей помещений разных замков;

наличие корпоративного межсетевого экрана (FireWall);

наличие антивирусной защиты и анти-спам фильтра;

контроль и управление учетными записями в домене;

ограничение доступа пользователей к ресурсам сети Интернет;

наличие установленных паролей доступа на ПЭВМ пользователей;

разграничение прав доступа в ОС;

наличие антивирусных средств на ПЭВМ пользователей;

наличие блокировки ОС при простое с последующим обязательным вводом пароля для разблокировки системы;

использование шифровальных (криптографических) средств для защиты ПДн при передаче их по каналам связи;

разграничение доступа к электронным документам, хранящимся как на ПЭВМ пользователей, так и на серверах;

разграничение доступа сотрудников к работе в ЛВС Музея в соответствии с назначенными правами и полномочиями;

наличие парольной защиты при доступе к АИС;

разграничение прав доступа сотрудников к информации и функциям в АИС в соответствии с назначенными правами и полномочиями;

регистрация событий;

периодический отбор и удаление из БД информации, содержащей ПДн, утратившей актуальность;

плановое резервное копирование БД, содержащих ПДн, и ограничение доступа к этим архивам.

2.3. Требования по обеспечению безопасности ПДн.

Каждый сотрудник Музея, участвующий в процессах обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным АИС, несет персональную ответственность за свои действия и обязан:

Выполнять требования всех внутренних документов Музея, касающихся информационной безопасности и порядку обработки ПДн.

Соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АИС.

Знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции.

Хранить в тайне свои аутентификационные реквизиты доступа.

Соблюдать установленные правила обращения и хранения персональной ключевой дискеты.



ПРАВИТЕЛЬСТВО МОСКВЫ

Отключать монитор своего персонального компьютера или блокировать вход в информационную систему в случае отлучения от своего рабочего места во время рабочего дня в целях защиты от просмотра данных посторонними лицами, включая работников других подразделений.

Выключать свою ПЭВМ после окончания рабочего дня.

Закрывать двери рабочих кабинетов на ключ в случае ухода из помещения в течение рабочего дня всех сотрудников. Также закрывать двери кабинетов после окончания рабочего дня.

2.4. Сотрудникам Музея запрещается:

Осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц.

Обсуждать ПДн с другими работниками Музея или иными лицами, не имеющими отношение к ПДн.

Записывать и хранить ПДн на неучтенных носителях информации (диски, дискеты, флэш-накопители и другие съемные устройства).

Оставлять без личного присмотра электронные носители и распечатки, содержащие ПДн.

Оставлять включенной без присмотра свою ПЭВМ, не предприняв необходимых мер защиты (отключение монитора, блокировка ОС, отключение ПЭВМ).

Покидать свое рабочее место, оставляя без присмотра посторонних лиц рядом с носителями, содержащими сведения о ПДн, включая работников других подразделений Музея.

## 3. Контроль за обработкой ПДн. Ответственность за выполнение требований настоящего Положения

Контроль за соблюдением требований данного Положения осуществляет администратор безопасности в виде просмотра и анализа отчетов, предоставляемых руководителями структурных подразделений при выявлении нарушений требований настоящего Положения.

Сотрудники, виновные в нарушении требований настоящего Положения, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.



ПРАВИТЕЛЬСТВО МОСКВЫ