ПОЛИТИКА В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ФЕДЕРАЛЬНОМ ГОСУДАРСТВЕННОМ БЮДЖЕТНОМ УЧРЕЖДЕНИИ КУЛЬТУРЫ «ГОСУДАРСТВЕННЫЙ МУЗЕЙНО-ВЫСТАВОЧНЫЙ ЦЕНТР «РОСИЗО», УРАЛЬСКИЙ ФИЛИАЛ ГОСУДАРСТВЕННОГО МУЗЕЙНО-ВЫСТАВОЧНОГО ЦЕНТРА «РОСИЗО»

1. ВВЕДЕНИЕ

1.1. Важнейшим условием реализации целей деятельности в Уральском филиале Государственного музейно-выставочного центра «РОСИЗО» (далее «Уф РОСИЗО») либо Оператор) является обеспечение необходимого и достаточного уровня информационной безопасности информации, к которой, в том числе, относятся персональные данные.

1.2. Политика в отношении обработки персональных данных в Уф РОСИЗО (далее – Положение) определяет порядок сбора, хранения, передачи и иных видов обработки персональных данных в Уф РОСИЗО (далее – Организация), а также сведения о реализуемых требованиях к защите персональных данных.

1.3. Политика разработана в соответствии с действующим законодательством РФ.

1.4. Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных). Детальный перечень персональных данных фиксируется в локальной нормативной документации Уф РОСИЗО.

1.5. Все обрабатываемые Уф РОСИЗО персональные данные являются конфиденциальной, строго охраняемой информацией в соответствии с законодательством.

Настоящая Политика проводится Уф РОСИЗО в отношении обработки и обеспечения защиты персональных данных (далее по тексту – настоящая Политика) физических лиц (субъектов персональных данных) на основании статьи 24 Конституции РФ, главы 14 Трудового кодекса РФ, Федерального закона от 27.07.2006 N 152-ФЗ (в редакции от 21.07.2014) "О персональных данных", Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 13.07.2015) "Об информации, информационных технологиях и о защите информации", других нормативных актов РФ, Приказа 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».

Цель Политики заключается в обеспечении безопасности объектов защиты Организации от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных, а также доведении до лиц, предоставляющих свои персональные данные необходимой информации, позволяющей оценить, какие персональные данные и с какими целями обрабатываются Организацией, какие методы обеспечения их безопасности реализуются.

Политика обеспечивает защиту прав и свобод субъектов при обработке их персональных данных с использованием средств автоматизации или без использования таких средств, а также устанавливает ответственность лиц, имеющих доступ к персональным данным, за невыполнение требований, регулирующих обработку и защиту персональных данных.

Настоящая Политика может быть изменена при изменении действующего законодательства РФ.

2. Перечень субъектов ПЕРСОНАЛЬНЫХ ДАННЫХ

Политика применяется в отношении всех персональных данных, которые могут быть получены Организацией в процессе деятельности, в том числе клиентов Организации.

3. Перечень персональных данных, обрабатываемых в Уф РОСИЗО

Перечень персональных данных, подлежащих защите определен в соответствии с законодательством Российской Федерации, нормативными и локальными актами Уф РОСИЗО и представлен в настоящих Правилах.
Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, в Уф РОСИЗО не осуществляется.

4. Функции Общества при осуществлении обработки ПД

УФ РОСИЗО при осуществлении обработки персональных данных:
- принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации, нормативных актов УФ РОСИЗО и локальных нормативных актов УФ РОСИЗО в области персональных данных;
- принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;
- назначает лицо, ответственное за организацию обработки персональных данных в УФ РОСИЗО;
- издает локальные и нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в УФ РОСИЗО;
- осуществляет ознакомление работников УФ РОСИЗО, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации, нормативных и локальных актов УФ РОСИЗО» в области персональных данных, в том числе требованиями к защите персональных данных, и обучение указанных работников;
- публикует или иным образом обеспечивает неограниченный доступ к настоящей Политике;
- сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации;
- прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации в области персональных данных;
- совершает иные действия, предусмотренные законодательством Российской Федерации в области персональных данных. Клиенты, используя сервисы, услуги Организации, сообщив Организации свои персональные данные, в том числе при посредничестве третьих лиц, признают своё согласие на обработку персональных данных в соответствии с настоящей Политикой.

5. УСЛОВИЯ ОБРАБОТКИ ПДН, ПЕРЕДАЧА (ПРЕДОСТАВЛЕНИЕ. ДОСТУП) ПДН РАБОТНИКОВ И ДРУГИХ СУБЪЕКТОВ ПДН.

Обработка персональных данных в УФ РОСИЗО осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.
УФ РОСИЗО без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.
УФ РОСИЗО вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

В целях внутреннего информационного обеспечения УФ РОСИЗО может создавать внутренние справочные материалы, в которые с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации, могут включаться его фамилия, имя, отчество, место работы, должность, год и место рождения, адрес, абонентский номер, адрес электронной почты, иные персональные данные, сообщаемые субъектом персональных данных.
Доступ к обрабатываемым в УФ РОСИЗО» персональным данным разрешается только работникам УФ РОСИЗО, занимающим должности, включенные в Приказ должностей структурных подразделений УФ РОСИЗО, при замещении которых осуществляется обработка персональных данных.
Согласие на обработку персональных данных может быть отозвано субъектом персональных данных. В случае отзыва субъектом персональных данных согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия субъекта персональных данных при наличии оснований, указанных действующим законодательством

6. СРОКИ ОБРАБОТКИ И ХРАНЕНИЯ ПДН.

Персональные данные Клиентов обрабатываются и хранятся в информационных системах и на бумажных носителях в Организации.
Персональные данные Клиентов хранятся в электронном виде: в локальной компьютерной сети Организации, в электронных папках и файлах в ПК работников, допущенных к обработке персональных данных Клиентов.
Хранение персональных данных Клиента может осуществляться не дольше, чем этого требуют цели обработки, если иное не предусмотрено федеральными законами РФ.
Сроки хранения персональных данных указаны в Приложении №1 (Перечень персональных данных)
В течение срока хранения персональные данные не могут быть обезличены или уничтожены.
По истечении срока хранения персональные данные могут быть обезличены в информационных системах и уничтожены на бумажном носителе в порядке установленном в Положении и действующем законодательстве РФ. (Акт об уничтожении персональных данных)

7. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКОВ ОБЩЕСТВА И ДРУГИХ СУБЪЕКТОВ ПДН

В соответствии с ст. 14 152 ФЗ «О персональных данных» Субъекты персональных данных имеют право на:
- полную информацию об их персональных данных, обрабатываемых в УФ РОСИЗО
- доступ к своим персональным данным, включая право на получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных федеральным законом;
- уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки;
- отзыв согласия на обработку персональных данных;
- принятие предусмотренных законом мер по защите своих прав;
- обжалование действия или бездействия УФ РОСИЗО осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или в суд;
- осуществление иных прав, предусмотренных законодательством Российской Федерации.

8. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ЗАКОНОДАТЕЛЬСТВА РФ В ОБЛАСТИ ПДН

Контроль за соблюдением структурными подразделениями УФ РОСИЗО законодательства Российской Федерации, нормативных и локальных актов УФ РОСИЗО в области персональных данных, в том числе требований к защите персональных данных, осуществляется с целью проверки соответствия обработки персональных данных, направленных на предотвращение и выявление нарушений законодательства Российской Федерации в области персональных данных, выявления возможных каналов утечки и несанкционированного доступа к персональным данным, устранения последствий таких нарушений.
Внутренний контроль за соблюдением структурными подразделениями администрации УФ РОСИЗО законодательства Российской Федерации, нормативных и локальных актов УФ РОСИЗО в области персональных данных, в том числе требований к защите персональных данных, осуществляется лицом, ответственным за организацию обработки персональных данных УФ РОСИЗО
Персональная ответственность за соблюдение требований законодательства Российской Федерации, нормативных и локальных актов УФ РОСИЗО в области персональных данных в структурном подразделении УФ РОСИЗО, а также за обеспечение конфиденциальности и безопасности персональных данных в указанных подразделениях УФ РОСИЗО возлагается на руководителей этих подразделений.

9. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.
Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).
Администратор информационных систем и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.
При нарушениях сотрудниками Организации, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.
Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях Организации, осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников Организации.
Необходимо внести в Положения о подразделениях Организации, осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

10. ПРИЛОЖЕНИЯ/СПИСОК ЛОКАЛЬНЫХ ДОКУМЕНТОВ.

Перечень персональных данных, обрабатываемых в УФ РОСИЗО.

11. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:
1. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.

2. «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденное Постановлением Правительства РФ от 17.11.2007 г. № 781.
3. «Порядок проведения классификации информационных систем персональных данных», утвержденный совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи РФ № 20 от 13.02.2008 г.
4. «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.
5. «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных си-стем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.
6. Нормативно-методические документы Федеральной службы по тех-ническому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:
7 Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
8. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
9. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
10. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП).

Перечень персональных данных, обрабатываемых в Уф РОСИЗО

Наименование (вид) ПДн	**Содержание персональных данных**	**Категории ПДн**	**Источник получения**	**Основание для обработки ПДн**	**Технологический процесс, использующий вид ПДн**	**Срок хранения, условия прекращения обработки**	**Общедоступность**
Первичные учетные данные клиента	ФИО клиента	4 категория	Субъект ПДн, договор	- Условия договора	- Заключение договора с клиентом - Расторжение договора с клиентом	3 года после расторжения договора*	Не общедоступные
Сведения о реквизитах клиента	- адрес эл. почты-адрес проживания/доставки - номер телефона	3 категория	Субъект ПДн, договор	- Условия договора	- Заключение договора с клиентом - Расторжение договора с клиентом	3 года после расторжения договора*	Не общедоступные

* Категория 3 – персональные данные, позволяющие идентифицировать субъекта ПДн. Категория 4 – обезличенные и (или) общедоступные персональные данные.