

**Автономная некоммерческая организация высшего образования  
«Университет мировых цивилизаций имени В.В. Жириновского»  
(АНО ВО «УМЦ»)**

**ПРИНЯТО**

на заседании Ученого Совета  
протокол от 29.06.2017 № 09

**УТВЕРЖДАЮ:**

Ректор Слоботчиков О.Н.  
30.06.2017

(внесены изменения в соответствии с приказом  
АНО ВО «УМЦ» от 16.01.2023 № 01)

(внесены изменения в соответствии с приказом  
АНО ВО «УМЦ» от 19.12.2024 № 400)

Ректор АНО ВО «УМЦ»  
\_\_\_\_\_ О.Н. Слоботчиков

**ПОЛОЖЕНИЕ  
О ПОРЯДКЕ РАБОТЫ С ПЕРСОНАЛЬНЫМИ  
ДАНЫМИ РАБОТНИКОВ УНИВЕРСИТЕТА**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящим Положением определяется порядок обработки персональных данных работников и обучающихся Автономной некоммерческой организации высшего образования «Университет мировых цивилизаций имени В.В. Жириновского» (далее – Университет).

1.2. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества Университета и работников.

## 2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Для целей настоящего Положения используются следующие основные понятия:

2.1.1. персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

2.1.2. персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Российским законодательством (далее - персональные данные, разрешенные для распространения) (п. 1.1. ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

2.1.3. оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (п. 2 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

2.1.4. обработка персональных данных работника - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

2.1.5. распространение персональных данных - действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

2.1.6. предоставление персональных данных - действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

2.1.7. блокирование персональных данных - временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

2.1.8. уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников (п. 8 ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»);

Автономная некоммерческая организация высшего образования  
«Университет мировых цивилизаций имени В.В. Жириновского»  
(АНО ВО «УМЦ»)

2.1.9. обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику (п. 9 ст. 3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

2.1.10. информационная система персональных данных - совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств, то есть вручную оператором.

2.2. Если иное не установлено Трудовым кодексом РФ, другими федеральными законами, при заключении трудового договора лицо, поступающее на работу, предъявляет работодателю:

2.2.1. паспорт или иной документ, удостоверяющий личность;

2.2.2. трудовую книжку и (или) сведения о трудовой деятельности (СТД-Р или СТД-ПФР), за исключением случаев, когда договор заключается впервые;

2.2.3. документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;

2.2.4. документы воинского учета - для военнообязанных и лиц, подлежащих призыву на военную службу;

2.2.5. документ об образовании и (или) квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;

2.2.6. справку, выданную органами МВД России, о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям (при поступлении на работу, к выполнению которой в соответствии с Трудовым кодексом РФ или иным федеральным законом не допускаются лица, имеющие или имевшие судимость, подвергающиеся или подвергавшиеся уголовному преследованию) (п. 6, 7 Административного регламента Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по выдаче справок о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования, утвержденного Приказом МВД России от 27.09.2019 № 660);

2.2.7. справку, выданную органами МВД России, о том, является или не является лицо подвергнутое административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ, - при поступлении на работу, к которой в соответствии с федеральными законами не допускаются лица, подвергнутые такому наказанию до окончания срока, в течение которого они считаются подвергнутыми административному наказанию (п. п. 13, 14 Административного регламента Министерства внутренних дел Российской Федерации по предоставлению государственной услуги по выдаче справок о том, является или не является лицо подвергнутое административному наказанию за потребление наркотических средств или психотропных веществ без назначения врача либо новых потенциально опасных психоактивных веществ, утвержденного Приказом МВД России от 02.11.2020 № 746);

2.2.8. дополнительные документы – в отдельных случаях, предусмотренных Трудовым кодексом РФ, иными федеральными законами, указами Президента РФ и постановлениями Правительства РФ.

2.3. В отделе по работе с персоналом Университета создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.3.1. Документы, содержащие персональные данные работников:

2.3.1.1. комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении;

2.3.1.2. комплекс материалов по анкетированию, тестированию, проведению собеседований с кандидатом на должность;

2.3.1.3. подлинники и копии приказов (распоряжений) по кадрам;

2.3.1.4. личные дела, трудовые книжки, сведения о трудовой деятельности работников (СТД-Р);

- 2.3.1.5. дела, содержащие материалы аттестаций работников;
- 2.3.1.6. дела, содержащие материалы внутренних расследований;
- 2.3.1.7. справочно-информационный банк данных по персоналу (картотеки, журналы);
- 2.3.1.8. подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Университета, руководителям структурных подразделений;
- 2.3.1.9. копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.
- 2.3.2. Документация по организации работы структурных подразделений:
  - 2.3.2.1. положения о структурных подразделениях;
  - 2.3.2.2. должностные инструкции работников;
  - 2.3.2.3. приказы, распоряжения, указания руководства Университета;
  - 2.3.2.4. документы планирования, учета, анализа и отчетности по вопросам кадровой работы.

### **3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ**

3.1. Источником информации обо всех персональных данных работника является непосредственно работник. Если персональные данные возможно получить только у третьей стороны, то работник должен быть заранее в письменной форме уведомлен об этом и от него должно быть получено письменное согласие. Работодатель обязан сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение. До начала обработки персональных данных работодатель обязан уведомить Роскомнадзор о своем намерении осуществлять их обработку.

3.2. Работодатель не имеет права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных Трудовым кодексом РФ и другими федеральными законами.

3.2.1. Обработка персональных данных, разрешенных для распространения, из числа специальных категорий персональных данных, указанных в ч. 1 ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», допускается, если соблюдаются запреты и условия, предусмотренные ст. 10.1 указанного Закона.

3.3. Работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом Российской Федерации или иными федеральными законами.

3.4. Обработка персональных данных работников работодателем возможна только с их согласия. Исключения составляют случаи, предусмотренные законодательством РФ (в частности, согласие не требуется при наличии оснований и соблюдении условий, перечисленных в п. 2 - 11 ч. 1 ст. 6, п. п. 2.1 - 10 ч. 2 ст. 10, ч. 2 ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

3.5. Согласие на обработку персональных данных должно быть конкретным, предметным, информированным, сознательным и однозначным (ч. 1 ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»). Письменное согласие работника на их обработку должно включать в себя, в частности, сведения, указанные в п. 1 - 9 ч. 4 ст. 9 названного Закона.

3.5.1. Если предоставление персональных данных и (или) получение работодателем согласия на их обработку являются обязательными, он должен разъяснить работнику юридические последствия отказа их предоставить и (или) дать согласие на обработку.

3.6. Письменное согласие работника на обработку персональных данных, разрешенных для распространения, оформляется отдельно от других согласий на обработку его персональных данных. При этом соблюдаются условия, предусмотренные, в частности, ст. 10.1 Федерального

закона от 27.07.2006 № 152-ФЗ «О персональных данных». Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения, утверждены Приказом Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения».

3.6.1. Письменное согласие на обработку персональных данных, разрешенных для распространения, работник предоставляет работодателю лично либо в форме электронного документа, подписанного электронной подписью с использованием информационной системы Роскомнадзора.

3.6.2. Работодатель обязан не позднее трех рабочих дней с момента получения указанного согласия опубликовать информацию об условиях обработки, о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных для распространения.

3.6.3. Согласие на обработку персональных данных, разрешенных для распространения, прекращает свое действие с момента поступления работодателю требования, указанного в п. 5.2.5 настоящего Положения.

3.7. Работник Университета представляет в отдел по работе с персоналом достоверные сведения о себе. Отдел по работе с персоналом проверяет достоверность сведений.

3.8. В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника должны соблюдать, в частности, следующие общие требования:

3.8.1. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией РФ, Трудовым кодексом РФ и иными федеральными законами.

3.8.2. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.8.3. Защита персональных данных работника от неправомерного их использования, утраты обеспечивается работодателем за счет его средств в порядке, установленном Трудовым кодексом РФ и иными федеральными законами. Работодатель обязан взаимодействовать с госсистемой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, в частности сообщать о компьютерных инцидентах, из-за которых произошла неправомерная передача (предоставление, распространение, доступ) персональных данных.

3.8.4. Работники и их представители должны быть ознакомлены под расписку а также об их правах и обязанностях в этой области.

3.8.5. Работники не должны отказываться от своих прав на сохранение и защиту тайны.

Заключаемый с работником договор не может содержать положения, которые ограничивают его права и свободы, устанавливают случаи обработки персональных данных несовершеннолетних (если иное не предусмотрено законодательством Российской Федерации), а также допускают в качестве условия заключения договора бездействие работника.

#### **4. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ**

4.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

4.1.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных Трудовым кодексом Российской Федерации или иными федеральными законами.

4.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения

товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

4.1.3. Предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждение того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное правило не распространяется на обмен персональными данными работников в порядке, установленном Трудовым кодексом РФ и иными федеральными законами.

4.1.4. Осуществлять передачу персональных данных работников в пределах Университета в соответствии с настоящим Положением, с которым работники должны быть ознакомлены под подпись.

4.1.5. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретной функции.

4.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

4.1.7. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функции.

4.2. Установленные работником запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме получения доступа) персональных данных, разрешенных для распространения, не действуют в случаях обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством РФ.

4.3. Персональные данные работников обрабатываются и хранятся в отделе по работе с персоналом.

4.4. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде (посредством локальной компьютерной сети).

4.5. При получении персональных данных не от работника (за исключением случаев, предусмотренных ч. 4 ст. 18 Федерального закона от 27.07.2006 № 152-ФЗ "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- перечень персональных данных;
- предполагаемые пользователи персональных данных;
- установленные Федеральным законом от 27.07.2006 № 152-ФЗ права субъекта персональных данных;
- источник получения персональных данных.

## 5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ РАБОТНИКОВ

5.1. Доступ к персональным данным работников предоставляется в строгом соответствии с принципом нераспространения персональных данных работников (определенные работники Университета имеют доступ лишь к тем персональным данным работников, которые необходимы для осуществления уставной деятельности и (или) соблюдения действующего законодательства Российской Федерации).

5.1.2. Право доступа к персональным данным работников имеют работники

Университета, которым предоставлен соответствующий доступ к определенным персональным данным в соответствии с выполняемой работой. Перечень должностей работников, которым предоставлен доступ к определенным персональным данным работников утверждается соответствующим приказом Ректора Университета, который разрабатывается в соответствии с настоящим Положением и нормами действующего законодательства Российской Федерации.

5.1.3. Безусловный доступ к персональным данным работников в силу занимаемой должности имеет Ректор Университета, как единоличный исполнительный орган Университета как юридического лица.

5.2. Работник Университета, в частности, имеет право:

5.2.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копии любой записи, содержащей его персональные данные, за исключением случаев, предусмотренных федеральным законом.

5.2.2. Требовать от работодателя исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Трудового кодекса РФ или иного федерального закона. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения.

5.2.3. Получать от работодателя сведения о наименовании и месте нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона.

5.2.4. Требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2.5. Получать информацию о способах исполнения работодателем обязанностей, предусмотренных ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ "Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

5.2.6. Требовать прекратить в любое время передачу (распространение, предоставление, доступ) персональных данных, разрешенных для распространения. Требование оформляется в письменном виде. Оно должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) работника, а также перечень персональных данных, обработка которых подлежит прекращению.

5.2.7. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия работодателя при обработке и защите его персональных данных.

## **6. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ**

6.1. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

6.2. Моральный вред, причиненный работнику вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 № 152-ФЗ "Об утверждении требований к содержанию согласия на обработку персональных данных,

разрешенных субъектом персональных данных для распространения, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работником убытков.

## 7. ИНФОРМАЦИОННЫЕ СИСТЕМЫ

7.1. Класс (классы) защищенности информационной системы (информационных систем) устанавливаются в Университете согласно Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных»

7.2. Университет использует следующие информационные системы персональных данных (типовые и специальные):

- корпоративная электронная почта;
- система электронного документооборота;
- система нормативно-справочной информации;
- система управления персоналом;
- информационно-обучающий портал.

Университет использует следующие системы защиты информационных систем персональных данных:

- антивирус – программное обеспечение, предназначенное для защиты компьютерных систем от вредоносных программ, таких как вирусы, трояны, шпионские программы и другие угрозы, антивирусный программный комплекс внедрен в Университет для мониторинга и обнаружения потенциальных угроз, а также для их удаления или изоляции;

- средство защиты от несанкционированного доступа Secret Net Studio, который позволяет осуществлять защиту сразу по многим направлениям, в функционал решения которого входит защита рабочих станций и серверов от вирусов, сетевых атак и вредоносных программ; обеспечение безопасного обмена данными с удаленными рабочими станциями, а также защита информации от утечек, несанкционированного доступа;

- межсетевой экран, позволяющий защитить сеть от DDOS-атак, вирусов, хакерских шпионских программ.

7.3. Система защиты персональных данных на бумажных носителях реализуется путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Персональные данные на бумажных носителях, находящиеся в делопроизводстве структурного подразделения Оператора, осуществляющего работу с субъектами персональных данных, могут находиться на рабочих столах или в специальных папках только в течение рабочего дня. По окончании рабочего дня данные документы должны убираться в запирающиеся на ключ сейфы (металлические шкафы), оборудованные внутренними замками. В случае, если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

Хранение персональных данных в неавтоматизированном виде:

- резюме, анкеты, документы, связанные с процессами по подбору персонала, хранятся в отделе кадров;
- личные дела работников, трудовые книжки и другие документы по кадровому делопроизводству хранятся в отделе кадров в запираемых шкафах;
- копии личных медицинских книжек работников, данные о сертификатах обязательных вакцинаций, и заключения медицинского учреждения о прохождении предварительного или периодического медицинского осмотра работников хранятся у заведующего медицинским кабинетом в запираемом шкафу;

Здание оператора оснащено техническими средствами охраны с постоянным

присутствием сотрудников. Вход в здание ограничен, осуществляется идентификация работников и иных лиц, входящих в здание оператора по электронным картам и документам, удостоверяющим личность. Помещения, где хранятся документы содержащие персональные данные работников, оснащаются металлическими шкафами и сейфами с возможностью физического запираания средств накопителей документов, содержащих персональные данные работников.

7.4. Конкретный порядок и условия доступа к информационным системам устанавливается приказом ректора Университета по предложению проректора по цифровизации образования и информационным технологиям.

7.5. Лицом, ответственным за определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных и применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных является проректор по цифровизации образования и информационным технологиям.

## 8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящие Положение вступает в силу с момента его утверждения приказом ректора Университета и действует вплоть до его отмены или принятия Положения в новой редакции.

8.2. В случае изменения действующего законодательства Российской Федерации, нормы, содержащиеся в настоящем Положении, которые не соответствуют таким изменениям, Университетом не применяются, а само Положение подлежит соответствующему изменению в разумные сроки, в соответствии с порядком разработки, принятия и утверждения локальных нормативных актов в Университете.

Представитель коллектива работников АНО ВО «УМЦ»:

\_\_\_\_\_ « \_\_\_\_\_ » \_\_\_\_\_ 20 \_\_\_\_ г.

