Государственное образовательное учреждение
высшего профессионального образования
РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
(РУДН)

УТВЕРЖДЕНО
Приказом Ректора РУДН
№ 214 от «30» МАР 2009 2009 г.

ПОЛОЖЕНИЕ

о защите, хранении, обработке и передаче персональных данных субъектов персональных данных в государственном образовательном учреждении высшего профессионального образования «Российский университет дружбы народов»

Настоящее Положение разработано в соответствии с Конституцией РФ, Трудовым кодексом РФ, Федеральным законом от 27.07.06 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.06 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 13.01.96 № 12-ФЗ «Об образовании», Федеральным законом от 22.08.96 № 125-ФЗ «О высшем и послевузовском профессиональном образовании», Федеральным законом от 22.10.04 № 125-ФЗ «Об архивном деле в Российской

системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

2. Общие положения

Цель настоящего Положения – защита прав Субъекта персональных данных (далее – «Субъекта») и его персональной информации в государственном образовательном учреждении высшего профессионального образования «Российский университет дружбы народов» (РУДН) от неправомерного использования, несанкционированного доступа и разглашения. Персональные данные являются конфиденциальной, строго охраняемой информацией.

Обработка персональных данных осуществляется Оператором исключительно в целях содействия Субъекту в трудоустройстве, обучении и продвижении по службе, законном представительстве, обеспечения личной безопасности, контроля качества и количества выполняемой работы, оплаты труда, обеспечения сохранности имущества, пользования льготами, предусмотренными законодательством РФ, локальными нормативными актами в соответствии с Уставом РУДН.

3. Права и обязанности Оператора при обработке персональных данных

3.1. В предусмотренных законодательством РФ случаях Оператор вправе уточнять (изменять, дополнять), блокировать и уничтожать персональные данные.

3.2. Оператор не имеет права:

3.2.1. Получать и обрабатывать персональные данные Субъекта о его политических, религиозных и иных убеждениях и частной жизни без его письменного согласия.

3.2.2. Получать и обрабатывать персональные данные Субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.2.3. Основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или из внешнего электронного информационного ресурса, при принятии решений, затрагивающих интересы Субъекта.

3.3. Оператор обязан:

3.3.1. Сообщить Субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа Субъекта дать письменное согласие на их получение.

3.3.2. Предпринять предусмотренные законодательством РФ меры для защиты конфиденциальности полученных персональных данных

3.3.3. Предоставлять соответствующую информацию по требованию Субъекта или его законного представителя, а также уполномоченного органа по защите прав субъектов персональных данных.

3.3.4. Прекратить обработку и уничтожить собранные персональные данные в случае:

3.3.4.1. достижения целей обработки или при утрате необходимости в их достижении;

3.3.4.2. требования Субъекта или уполномоченного органа по защите прав субъектов персональных данных - если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

3.3.4.3. невозможности устранить допущенные нарушения в отношении обработки персональных данных в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными;

3.3.4.4. отзыва Субъектом согласия на обработку своих персональных данных.

3.3.5. Уведомлять уполномоченный орган по защите прав субъектов персональных данных об изменениях сведений об Операторе.

3.3.6. При передаче персональных данных Субъекта другим юридическим и физическим лицам соблюдать следующие требования:

3.3.6.1. Не сообщать персональные данные третьей стороне без письменного согласия Субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в случаях, установленных федеральными законами.

3.3.6.2. Не сообщать персональные данные Субъекта в коммерческих целях без его письменного согласия.

3.3.6.3. Предупреждать лиц, получающих персональные данные Субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные Субъекта, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными Субъектов в порядке, установленном федеральными законами.

3.3.6.4. Не запрашивать информацию о состоянии здоровья Субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения им трудовой функции.

3.3.6.5. Передавать персональные данные представителям Субъекта в порядке, установленном законодательством РФ, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций.

4. Права и обязанности Субъекта персональных данных в целях обеспечения защиты персональных данных, хранящихся у Оператора.

4.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, Субъекты имеют право:

4.1.1. Принять решение о предоставлении персональных данных и согласиться на их обработку своей волей и в своем интересе, за исключением случаев, предусмотренных законодательством РФ.

4.1.2. Отозвать согласие на обработку персональных данных. Отзыв должен быть выражен в письменной форме в виде заявления и доставлен Оператору лично или заказным письмом.

4.1.3. Получать полную информацию о своих персональных данных и их обработке.

4.1.4. Свободного бесплатного доступа к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные Субъекта, за исключением случаев, предусмотренных федеральными законами. Получение указанной информации о своих персональных данных возможно при личном обращении Субъекта в соответствующие службы Оператора.

4.1.5. Требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением требований Российского законодательства. Указанное требование должно быть оформлено письменным заявлением Субъекта. В случае отказа Оператора исключить или исправить персональные данные Субъекта, Субъект имеет право заявить в письменном виде Оператору о своем несогласии, с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера Субъект имеет право дополнить заявлением, выражающим его собственную точку зрения.

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

4.1.7. Обжаловать в суде любые неправомерные действия или бездействия Оператора при обработке и защите его персональных данных.

4.2. В целях обеспечения достоверности персональных данных Субъекты обязаны:

4.2.1. При осуществлении правоотношений между Субъектом персональных данных и Оператором, предоставлять Оператору достоверные сведения о себе, в порядке и объеме, предусмотренном законодательством Российской Федерации.

4.2.2. В случае изменения персональных данных Субъекта: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения должностных, трудовых обязанностей и т.п.) сообщать об этом Оператору в течение 5 рабочих дней с момента их изменений.

5. Порядок сбора, обработки, хранения и передачи персональных данных.

5.1. Все персональные данные предоставляются Субъектом лично. Если персональные данные возможно получить только у третьей стороны, то Оператор обязан заранее уведомить об этом Субъекта и получить его письменное согласие.

5.2. Субъекты (работники Оператора) должны быть ознакомлены под роспись со своими правами и обязанностями при поступлении на работу, остальные субъекты должны быть ознакомлены со своими правами и обязанностями при даче письменного согласия на обработку и защиту своих персональных данных.

5.3. Персональные данные субъектов хранятся на бумажных и электронных носителях. Хранение персональных данных осуществляется по форме, позволяющей определить Субъекта, не дольше, чем этого требуют цели обработки.

5.4. В процессе хранения персональных данных должны обеспечиваться:

5.4.1. требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

5.4.2. сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящим Положением;

5.4.3. контроль над достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

5.5. Доступ к персональным данным Субъектов имеют сотрудники РУДН в соответствии с Положениями о структурных подразделениях и должностными инструкциями исключительно в целях, которые необходимы для выполнения конкретных функций.

5.6. Ответственным за организацию и осуществление хранения персональных данных является начальник соответствующего структурного подразделения РУДН. Он осуществляет контроль за хранением персональных данных в соответствии с требованиями к учету и хранению конфиденциальной информации.

6. Защита персональных данных без использования средств автоматизации

6.1. Персональные данные при их обработке без использования средств автоматизации должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков). Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории должен использоваться отдельный материальный носитель.

6.2. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы:

6.2.1. о факте обработки ими персональных данных, обработка которых осуществляется Оператором без использования средств автоматизации;

6.2.2. о категориях обрабатываемых персональных данных;

6.2.3. об особенностях и правилах осуществления такой обработки, установленных в соответствии с нормативными правовыми актами.

6.3. Оператор при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, соблюдает следующие условия:

6.3.1. типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) содержат:

- сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации;
- имя (наименование) и адрес Оператора;
- фамилию, имя, отчество и адрес Субъекта;
- источник получения персональных данных;
- сроки обработки персональных данных;
- перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
- общее описание используемых оператором способов обработки персональных данных;

6.3.2. типовая форма предусматривает поле, в котором Субъект ставит отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

6.3.3. типовая форма составлена таким образом, чтобы каждый из Субъектов, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, не нарушая прав и законных интересов иных Субъектов;

6.3.4. типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

6.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если он не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных.

6.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

6.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, если же такой способ не допустим в связи с техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

6.7. В целях обеспечения безопасности передачи персональных данных, обрабатываемых без использования средств автоматизации, устанавливаются следующие правила:

6.7.1. обработка персональных данных осуществляется таким образом, что в отношении каждой категории персональных данных можно определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

6.7.2. необходимо обеспечить раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

6.7.3. при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие

несанкционированный к ним доступ.

6.8. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Оператором.

7. Защита персональных данных при их обработке с использованием средств автоматизации.

7.1. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

7.2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных. Такая система включает:

7.2.1. организационные меры и средства защиты информации (в том числе шифровальные (криптографические)) средства;

7.2.2. средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных;

7.2.3. используемые в информационной системе информационные технологии.

7.3. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

7.4. Для обеспечения безопасности персональных данных при их обработке в информационной системе осуществляется защита речевой информации и информации, обрабатываемой техническими средствами. Также защите подлежит информация, представленная в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе.

7.5. Достаточность принятых мер по обеспечению безопасности персональных данных в информационных системах оценивается при проведении государственного контроля и надзора.

7.6. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

7.7. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

7.8. Информационные системы классифицируются Оператором в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности, в соответствии с порядком проведения классификации информационных систем.

7.9. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств.

7.10. Размещение информационных систем, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц. Для выполнения данных мероприятий должны обеспечиваться следующие условия:

7.10.1. Физический доступ ко всем информационным системам, содержащим

персональные данные, должен быть ограничен, и строго контролироваться во избежание несанкционированных изменений конфигурации, вывода оборудования из строя, хищения и т.п.

7.10.2. Все действия по техническому обслуживанию, ремонту и замене оборудования информационных систем проводятся исключительно с разрешения Оператора (руководителя структурного подразделения) и должны быть зарегистрированы в установленном порядке.

7.10.3. Все ремонтные и иные работы проводимые персоналом, не имеющим прав доступа в служебные помещения с информационными системами, должны проводиться только в сопровождении должностных лиц (работников) Оператора..

7.10.4. Носители информации на магнитной, оптической, твердотельной и бумажной основе, содержащие персональные данные, должны учитываться, храниться и уничтожаться в порядке, установленном для конфиденциальной информации.

7.10.5. Для исключения утечки информации, отчуждаемые магнитные, оптические и твердотельные носители информации должны пройти полную очистку. Если произвести очистку информации невозможно, то носители информации должны быть физически уничтожены.

7.10.6. По окончании обработки персональных данных в информационных системах, а также при передаче персональных данных Оператор обязан произвести стирание временных файлов на несъёмных носителях информации и информации в оперативной памяти. Одним из способов стирания информации в оперативной памяти является перезагрузка ЭВМ.

7.10.7. Перед передачей оборудования информационных систем необходимо полностью удалить всю конфиденциальную информацию.

7.10.8. Во избежание потери персональных данных, ЭВМ и серверы, содержащие персональные данные для постоянного хранения, должны быть обеспечены гарантированным бесперебойным электропитанием.

7.11. Безопасность персональных данных при их обработке в информационной системе обеспечивает Оператор.

7.12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают:

7.12.1. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

7.12.2. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

7.12.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

7.12.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

7.12.5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

7.12.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

7.12.7. учет лиц, допущенных к работе с персональными данными в информационной системе;

7.12.8. контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

7.12.9. рассмотрение и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности

персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

7.12.10. описание системы защиты персональных данных.

7.13. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного Оператором.

7.14. При обнаружении нарушения порядка предоставления персональных данных Оператор незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин и устранения последствий данного нарушения.

7.15. Перечень мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах может устанавливаться отдельными локальными нормативными актами Оператора.

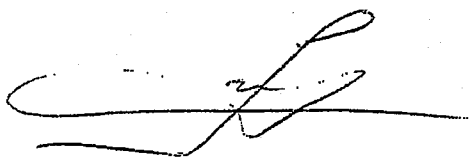
7.16. После прекращения трудового договора с лицом, имевшим доступ к персональным данным, необходимо лишать его прав доступа к внутренним информационным ресурсам РУДН, системам, сервисам и конфиденциальной информации путем оперативного изменения паролей, идентификаторов, ключей шифрования и т.п.

7.17. При переводе лица на другую должность его права доступа к информационной систем должны пересматриваться. При выходе сотрудника в долгосрочный отпуск приостанавливается действие всех прав доступа.

7.18. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 7.13. настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами контроля доступа информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется должностными лицами (работниками) Оператора.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.

Оператор, а также лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта персональных данных, установленных действующим законодательством Российской Федерации и настоящим Положением, привлекаются к дисциплинарной и материальной ответственности, а также несут гражданско-правовую, административную и уголовную ответственность, предусмотренную законодательством Российской Федерации.

Начальник УИТО  В.В.Шевцов

ЛИСТ СОГЛАСОВАНИЯ

Положения о защите, хранении, обработке и передаче
персональных данных субъектов персональных данных в
государственном образовательном учреждении высшего профессионального образования
«Российский университет дружбы народов»

Проект Положения вносит:

Управление информационно-технологического обеспечения РУДН

Начальник УИТО — Шевцов В.В. "__" _____ 2009

СОГЛАСОВАНО:

Первый Проректор -
Проректор по экономической деятельности — Щесняк Е.Л. "__" _____ 2009

Проректор по общим вопросам — Плотников А.В. "12" 05 2009

Главный юрисконсульт — Рогова Н.П. "16" марта 2009

Начальник Управления по работе
с персоналом и кадровой политики — Ковальчуков Н.А. "16" 03 2009

Главный бухгалтер — Зорин А.В. "24" 03 2009

Начальник ПФУ — Куринин И.Н. "23" 03 2009

Начальник Коммерческого управления — Должикова А.В. "19" 03 2009