МИНОБРНАУКИ РОССИИ

Федеральное государственное
бюджетное образовательное учреждение
высшего образования
**Российский государственный
гуманитарный университет»
(ФГБОУ ВО «РГГУ»)**

Приложение № 1

УТВЕРЖДЕНА
приказом РГГУ
от 31.01.2022 № 01-43/осн

Политика в области обработки

и защиты персональных данных

1. Общие положения

1.1. Политика РГГУ в области обработки и защиты персональных данных определяет основные принципы, цели и способы обработки персональных данных, а также требования к их защите.

1.2. РГГУ – государственное образовательное учреждение, поэтому формирование информационных потоков и обеспечение их эффективного функционирования в первую очередь связаны с учебным процессом. Обработка и защита персональных данных осуществляется для абитуриентов и обучающихся, а также преподавателей и работников подразделений Университета.

1.3. Обработка информации, отнесенной к персональным данным, и обеспечение ее защиты осуществляется в соответствии Конституцией РФ, Федеральными законами, постановлениями Правительства РФ и ФСТЭК России.

2. Основополагающие термины и определения

2.1. Персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу.

2.2. 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.

2.3. Обработка персональных данных - 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.

2.4. Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

2.5. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.6. Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.7. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.8. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.9. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.10. Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3. Принципы обработки персональных данных

3.1. Обработка персональных данных работников и обучающихся может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов - для содействия студентам в обучении, а работникам в трудовой деятельности.

3.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

3.3. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям.

3.4. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки.

3.5. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

4. Меры, применяемые для защиты персональных данных

4.1. РГГУ принимает необходимые и достаточные организационные и технические меры, предусмотренные законодательством в области защиты персональных данных, для защиты персональных данных, требующих обеспечения конфиденциальности, от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий с ними третьих лиц.

4.2. При поручении обработки персональных данных третьим лицам в поручении указываются требования к защите обрабатываемых персональных данных в соответствии с требованиями законодательства в области персональных данных.

4.3. Внутренний контроль за соответствием обработки персональных данных законодательству и принятым в соответствии с ним нормативным правовым актам осуществляется руководством РГГУ.

5. Обязанности работников по защите персональных данных

5.1. Регламентация доступа к конфиденциальным сведениям и к обработке персональных данных:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;

- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

- рациональное размещение рабочих мест сотрудников, при котором исключается бесконтрольное использование защищаемой информации;

- знание работниками требований в конкретном подразделении к обращению с конфиденциальными документами и защите информации;

- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;

- персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа;

- установление мест и условий хранения для материальных носителей персональных данных.

5.2. В структурных подразделениях РГГУ обработка и хранение персональных данных осуществляется в порядке, исключающем к ним физический или электронный доступ посторонних лиц.

5.3. Работник Университета, который, в связи с исполнением трудовых обязанностей имеет право доступа к персональным данным, обязан:

- выполнять требования организационно-распорядительных документов и инструкций конкретного подразделения по сбору, обработке и передаче персональных данных, а также хранению конфиденциальной информации;

- выполнять требования руководителя подразделения по порядку приема, учета и контроля деятельности посетителей;

- при уходе в отпуск, служебной командировке и иных случаях длительного отсутствия, работник обязан передать документы и иные носители, содержащие персональные данные, другому работнику, допущенному к их обработке – по письменному указанию руководителя структурного подразделения;

- при увольнении сдать документы и иные носители, содержащие персональные данные и другую информацию руководителю структурного подразделения или другому работнику - по письменному указанию руководителя структурного подразделения.

6. Меры, применяемые для защиты персональных данных, мониторинг работы информационных сетей

6.1. Делопроизводство, документооборот, неавтоматизированная и автоматизированная обработка данных осуществляются в Управлении кадров, Управлении бухгалтерского учета, экономики и финансов, Управлении по работе со студентами, Управлении профориентационной работы и организации приема, Учебно-методическом управлении, Управлении аспирантурой и докторантурой, Управлении по научной работе, Административно-правовом управлении, Отделе охраны и режима, Втором отделе, Отделе гражданской обороны и чрезвычайных ситуаций, Информационном комплексе «Научная библиотека», общежитиях, учебных структурных подразделениях.

6.2. Для работы с конфиденциальной информацией работник получает соответствующий доступ - разрешение на право работы с защищаемой информацией с учетом его должностных инструкций от руководителя подразделения РГГУ. При этом в его трудовой договор и должностную инструкцию вносятся положения о порядке работы и ответственности за работу с персональными данными.

6.3. Доступ сотрудников к работе в автоматизированных информационных системах осуществляется в соответствии с их должностными обязанностями. Регистрация пользователя выполняется системным администратором в соответствии с правами доступа к внутренним и внешним электронным информационным ресурсам.

6.4. Руководители структурных подразделений РГГУ, имеющих право разрешать доступ к автоматизированным информационным системам и наделять пользователей правами доступа, определяются отдельными распоряжениями.

6.5. Учет структурных подразделений и работников, имеющих доступ для работы с защищаемой информацией, ведет ответственное лицо, назначенное приказом РГГУ.

6.6. Положение «Об обработке и защите персональных данных работников, обучающихся и абитуриентов РГГУ» размещено на сайте РГГУ.

6.7. Подписание государственных контрактов и других документов с использованием ЭЦП осуществляется уполномоченными работниками РГГУ.

6.8. Сведения, необходимые для оформления студентам и аспирантам проездных билетов или получения различных льгот, подготавливаются в Управлении кадров и передаются в электронном виде в систему ГУП «Московский социальный регистр» с использованием ЭЦП.

6.9. Для работы с государственными учреждениями Управление по информатизации и ИТ обеспечивает защищенные каналы связи. Обязательная переаттестация защищенных каналов связи их техническая поддержка выполняются в соответствии со сроками и требованиями ФСТЭК и ФСБ России.

6.10. Технический мониторинг информационной безопасности автоматизированных систем РГГУ от несанкционированного доступа, распространения, искажения и утраты информации осуществляет Управление по информатизации и информационным технологиям.

6.11. Организационные и административные аспекты обеспечения информационной безопасности курирует проректор по безопасности.

6.12. Работник, по вине которого было допущено нарушение норм, регулирующих получение, обработку и защиту персональных данных, может быть привлечен к дисциплинарной и материальной, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7. Регистрация инцидента информационной безопасности и устранение его последствий

7.1. Мониторинг автоматизированных систем и нарушений информационной безопасности осуществляет Управление по информатизации и информационным технологиям.

7.2. Ответственными за выявление событий информационной безопасности и за реагирование на них, являются сотрудники, имеющие право доступа к информационным системам РГГУ в соответствии с должностными обязанностями.

7.3. Для устранения последствий и причин инцидента информационной безопасности создается специальная комиссия под председательством проректора по безопасности.

7.4. Каждый работник и обучающийся в РГГУ несет персональную дисциплинарную, административную или уголовную ответственность за действия либо бездействия, повлекшие неправомерное уничтожение, блокирование, модификацию либо копирование персональных данных, в соответствии с действующим законодательством Российской Федерации.