ГБОУ ВО «БАШКИРСКАЯ АКАДЕМИЯ ГОСУДАРСТВЕННОЙ СЛУЖБЫ И УПРАВЛЕНИЯ ПРИ ГЛАВЕ РЕСПУБЛИКИ БАШКОРТОСТАН»

ПРИКАЗ

31 марта 2022 г. № 133 А

г. Уфа

Об утверждении Положения об обработке персональных данных с использованием средств автоматизации

Во исполнение Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», в целях осуществления обработки персональных данных с использованием средств автоматизации ГБОУ ВО «БАГСУ, п р и к а з ы в а ю:

1. Утвердить Положение об обработке персональных данных с использование средств автоматизации, далее - «Положение», согласно приложению.
2. Канцелярии довести информацию до структурных подразделений.
3. Контроль исполнения требований настоящего Положения возложить на ответственное лицо за организацию обработки персональных данных в ГБОУ ВО «БАГСУ», начальника отдела информационно – технического обеспечения Степанова С.П.

Ректор Д.М. Абдрахманов

Приложение
к Приказу от 31.03.22 № 133-А

ПОЛОЖЕНИЕ
об обработке персональных данных с использование средств автоматизации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об обработке персональных данных с использованием средств автоматизации (далее – Положение) ГБОУ ВО «БАГСУ» разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 29.12.2012 № 273 – ФЗ «Об образовании в Российской Федерации», Политикой обработки и защиты персональных данных в ГБОУ ВО «БАГСУ» (далее - Политика обработки и защиты персональных данных), а также иными нормативно-правовыми актами в сфере защиты персональных данных, действующими на территории Российской Федерации.

1.2. Положение определяет порядок автоматизированной обработки персональных данных субъектов персональных данных, персональные данные которых подлежат обработке на основании полномочий ГБОУ ВО «БАГСУ».

1.3. Целью Положения является защита персональных данных субъектов персональных данных от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. **Информация** – сведения (сообщения, данные) независимо от формы их представления.

2.2. **Доступ к информации** – возможность получения информации и ее использования.

2.3. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.4. **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.

2.5. **Носитель персональных данных** – любой материальный объект или среда, используемый для хранения или передачи персональных данных.

2.6. **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.

2.7. **Субъект персональных данных** – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

2.8. **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.

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

2.10. **Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.11. **Контролируемая зона (КЗ)** – это пространство (территория, здание, часть здания, помещения), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

2.12. **Несанкционированный доступ (НСД)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

3. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка персональных данных в ГБОУ ВО «БАГСУ» может осуществляться исключительно в целях, указанных в Политике обработки и защиты персональных данных.

3.2. При определении объема и содержания обрабатываемых персональных данных работники ГБОУ ВО «БАГСУ» должны руководствоваться Политикой обработки и защиты персональных данных с учетом действующего законодательства Российской Федерации, а также настоящим Положением.

3.3. Обработка персональных данных с использованием средств автоматизации (автоматизированным способом) может осуществляться исключительно на автоматизированных рабочих местах, утверждённых Перечнем автоматизированных рабочих мест ИСПДн.

3.4. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в ГБОУ ВО «БАГСУ» определяется Политикой обработки и защиты персональных данных.

4. ПОРЯДОК ХРАНЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Хранение носителей персональных данных (магнитных, оптических, электронных) должно осуществляться в закрытых шкафах, сейфах, помещениях в порядке, исключающем доступ к ним третьих лиц.

4.2. Безопасность персональных данных при их обработке с использованием технических и программных средств обеспечивается с помощью системы защиты персональных данных, включающей в себя организационные меры и средства защиты информации,

удовлетворяющие устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

4.3. Обработка персональных данных ГБОУ ВО «БАГСУ» осуществляется до наступления одного из условий прекращения обработки персональных данных указанных в Политике обработки и защиты персональных данных.

4.4. По истечении срока хранения (30 дней, если иное не оговорено в нормативно-правовых актах) для носителей персональных данных допускается гарантированное удаление информации методом многократной перезаписи с помощью специализированных программ без уничтожения материального носителя.

4.5. ГБОУ ВО «БАГСУ» оставляет за собой право на обезличивание персональных данных.

5. ПОРЯДОК ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Передача персональных данных субъектов персональных данных допускается только тем работникам ГБОУ ВО «БАГСУ», которые имеют допуск к обработке персональных данных.

5.2. В целях соблюдения законодательства Российской Федерации для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных, ГБОУ ВО «БАГСУ» в ходе своей деятельности предоставляет персональные данные организациям, перечисленным в Политике обработки и защиты персональных данных.

5.3. Иное распространение персональных данных субъекта не допускается.

6. ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Защита персональных данных субъекта от неправомерного их использования, случайного доступа или утраты обеспечивается ГБОУ ВО «БАГСУ» за счет собственных ресурсов и средств.

6.2. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

6.2.1. Проведение организационных мероприятий:

6.2.1.1. разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данным;

6.2.1.2. ознакомление работников с законодательством Российской Федерации и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

6.2.1.3. организация учёта носителей персональных данных;

6.2.1.4. разработка модели угроз безопасности персональным данным;

6.2.1.5. проведение инструктажа работников по вопросам защиты персональных данных.

6.2.2. Программно-аппаратная защита:

6.2.2.1. внедрение программно-аппаратных средств защиты информации в соответствии с приказом ФСТЭК России от 25 декабря 2017 г. N 239 «Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

6.2.3. Инженерно-техническая защита:

6.2.3.1. установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

6.2.3.2. создание отдельных помещений с системой контроля доступа, в которых будут располагаться информационные системы персональных данных, установка сигнализации, видеонаблюдения, режима охраны здания.

6.3. Определение конкретных мер, общую организацию, планирование и контроль выполнения мероприятий по защите персональных данных осуществляет ответственный за организацию обработки персональных данных в соответствии с законодательством в области защиты персональных данных и локальными нормативно-правовыми актами ГБОУ ВО «БАГСУ».

6.4. Контроль за соблюдением правил защиты персональных данных в структурных подразделениях осуществляют их непосредственные руководители.

7. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

7.1. Допуск к персональным данным субъекта могут иметь только те работники ГБОУ ВО «БАГСУ», которым персональные данные необходимы в связи с исполнением ими своих трудовых обязанностей. Перечень таких работников содержится в «Списке лиц, доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей».

7.2. Процедура оформления допуска к персональным данным представляет собой следующую строгую последовательность действий:

7.2.1. ознакомление работника с настоящим Положением, Политикой обработки и защиты персональных данных, другими локальными нормативно-правовыми актами ГБОУ ВО «БАГСУ», касающимися обработки персональных данных;

7.2.2. истребование с работника Обязательства о неразглашении информации ограниченного доступа.

7.3. Каждый работник должен иметь доступ к минимально необходимому набору персональных данных субъектов, необходимых ему для выполнения служебных (трудовых) обязанностей.

7.4. Работникам, не имеющим надлежащим образом оформленного допуска, доступ к персональным данным субъектов запрещается.

8. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

8.1. Состав информационных систем ГБОУ ВО «БАГСУ» определяется Перечнем информационных систем.

8.2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

8.3. Безопасность персональных данных достигается 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.

8.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством Российской Федерации порядке.

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

8.6. Размещение информационных систем, специальное оборудование 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.

8.7. Безопасность персональных данных при их обработке в информационной системе обеспечивает специалист, ответственный за обеспечение безопасности персональных данных в информационных системах.

8.8. При обработке персональных данных в информационной системе должно быть обеспечено:

8.8.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

8.8.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

8.8.3. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

8.8.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8.8.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

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

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

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

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

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

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

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

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

8.9.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

8.9.9. разбирательство 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;

8.9.10. описание системы защиты персональных данных.

8.10. Иные требования по обеспечению безопасности информации и средств защиты информации в ГБОУ ВО «БАГСУ» выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти субъекта Российской Федерации, в котором находится Оператор.

9. ОТВЕТСТВЕННОСТЬ

9.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, ответственного за обеспечение безопасности персональных данных в информационных системах и ответственного за организацию обработки персональных данных в ГБОУ ВО «БАГСУ».

9.2. Работники ГБОУ ВО «БАГСУ», виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

9.2.1. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами ГБОУ ВО «БАГСУ», влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник ГБОУ ВО «БАГСУ», имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ГБОУ ВО «БАГСУ» (в соответствии с п.7 ст. 243 Трудового кодекса Российской Федерации).

9.2.2. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях Российской Федерации.

9.2.3. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса Российской Федерации.