GMAC Controller-to-Controller Data Protection Addendum

This GMAC Controller-to-Controller Data Protection Addendum ("**DPA**") supplements and forms part of the agreement that references and incorporates this DPA (the "**Agreement**") and sets forth the terms governing the Processing of De-Identified Data and GMAC Personal Data that is provided or made available by Graduate Management Admission Council ("**GMAC**") to the other party to the Agreement (the "**Recipient**") (GMAC and Recipient together, the "**Parties**" and each individually, a "**Party**") as part of the GMAC Services.

1. Definitions. Capitalized terms used but not defined herein have the meanings assigned in the Agreement. For the purposes of this DPA, the terms below have the following meanings whenever capitalized:

1.1. "**CCPA**" means the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., as amended from time to time, together with the regulations issued thereunder.

1.2. "**Controller**" means an entity that determines the purposes and means of the Processing of Personal Data, and includes the term "business" as that term is defined in the CCPA.

1.3. "**GMAC Personal Data**" means Personal Data that is disclosed or made available by GMAC to Recipient under the Agreement as part of GMAC's provision of the GMAC Services.

1.4. "**GMAC Services**" means the GMAC products, services, or other offerings provided by GMAC to Recipient under the Agreement that incorporates this DPA.

1.5. "**Data Protection Laws**" means any privacy or data security law, statute, ordinance, regulation, or governmental rule of any jurisdiction applicable to the Processing of GMAC Personal Data under the Agreement, including, as applicable and without limitation, (a) U.S. Privacy Laws and GDPR; and (b) any applicable regulations, codes of practice, or guidance pertaining to the Processing of Personal Data published by a relevant regulatory authority, in each case as amended from time to time.

1.6. "**De-Identified Data**" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, or a device linked to such a natural person, or that is otherwise considered "deidentified" or "de-identified data" under applicable Data Protection Laws.

1.7. "**EEA Restricted Transfer**" means a Transfer (or onward Transfer) by GMAC to the Recipient of GMAC Personal Data originating in the EEA or Switzerland that is subject to GDPR or the Swiss Federal Act on Data Protection, where any required adequacy means can be met by entering into the EU Standard Contractual Clauses.

1.8. "**EU Standard Contractual Clauses**" means the standard contractual clauses annexed to Commission Implementing Decision (EU) (2021/914) of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as currently set out at https://eurlex.europa.eu/eli/dec_impl/2021/914/oj.

1.9. "**GDPR**" means Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) and any European Union member state law implementing the same, and, for the purposes of this DPA, includes the corresponding Data Protection Laws of the United Kingdom, including UK GDPR and the Data Protection Act 2018.

1.10. "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. As used herein, the term "Personal Data" includes, but is not limited to, information defined as "personal information," "personally identifiable information," or other similar terms under applicable Data Protection Laws.

1.11. "**Processing**" means any operation or set of operations which is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

1.12. "**Processor**" means an entity that Processes Personal Data on behalf of a Controller, and includes the term "service provider" as that term is defined in the CCPA.

1.13. "**Security Incident**" means any actual or reasonably suspected unauthorized access to or acquisition, disclosure, use, alteration, or loss of GMAC Personal Data (including, without limitation, hard copy records), including, and without limitation, a "personal data breach" as defined by GDPR.

1.14. "**Transfer**" means to disclose or otherwise make Personal Data available, either by physical movement of the Personal Data, or by enabling remote access to the Personal Data.

1.15. "**UK Restricted Transfer**" means a transfer (or onward transfer) by GMAC to the Recipient of Personal Data originating in the United Kingdom that is subject to UK GDPR where any required adequacy means can be met by entering into the EU Standard Contractual Clauses and the UK Addendum.

1.16. "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses version B1.0, issued by the UK Information Commissioner's Office under S119A(1) Data Protection Act 2018 and in force as of 21 March 2022, as currently set out at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf, as revised by the UK Information Commissioner's Office from time to time in accordance therewith.

1.17. "**U.S. Privacy Laws**" means all U.S. laws, rules, regulations, directives, and government requirements and guidance, federal or state, currently in effect and as they become effective relating in any way to privacy, confidentiality, security, or consumer protection that apply to the Processing of GMAC Personal Data. U.S. Privacy Laws may include, but are not limited to, the CCPA; the Colorado Privacy Act, Colo. Rev. Stat. Ann. § 6-1-1301 et seq.; the Delaware Personal Data Privacy Act, Del. Code

Ann. tit. 6, § 12D-101 et seq.; the Maryland Online Data Privacy Act, Md. Code Ann., Com. Law § 14-4701 et seq.; the Minnesota Consumer Data Privacy Act, Minn. Stat. Ann. § 325O.01 et seq.; the New Jersey Data Protection Act, N.J. Stat. § 56:8-166.4 et seq.; and the Oregon Consumer Privacy Act, Or. Rev. Stat. Ann. § 646A.570 et seq., in each case including any regulations and guidance that may be issued thereunder.

2. Roles of the Parties; Processing of GMAC Personal Data.

2.1. The Parties acknowledge and agree that each Party is an independent Controller of GMAC Personal Data and will individually (and not jointly) determine the purposes and means of its Processing of GMAC Personal Data. The Recipient shall, notwithstanding the foregoing, Process GMAC Personal Data only for the limited purposes specified in, and subject to the restrictions set forth in, the Agreement and this DPA. The details of the Processing of GMAC Personal Data are set forth in Appendix 1 to this DPA.

2.2. The Recipient shall comply with applicable Data Protection Laws with respect to its Processing of GMAC Personal Data and shall provide a level of privacy protection for GMAC Personal Data consistent with the requirements of applicable Data Protection Laws. The Recipient shall promptly notify GMAC if it makes a determination that it can no longer meet its obligations under this DPA or comply with applicable Data Protection Laws. GMAC shall have the right, upon notice, including from the Recipient pursuant to the preceding sentence, to take reasonable and appropriate steps to help ensure that the Recipient Processes GMAC Personal Data in a manner consistent with GMAC's obligations under applicable Data Protection Laws, and to stop and remediate any unauthorized Processing of GMAC Personal Data.

2.3. Without limiting the generality of the foregoing, the Recipient shall:

a. provide all privacy notices required under applicable Data Protection Laws to the subjects of GMAC Personal Data with respect to its own Processing;

b. implement appropriate organizational and technical security measures prior to and during Processing of GMAC Personal Data to protect against the accidental, unlawful, or unauthorized access to or use, transfer, destruction, loss, alteration, commingling, disclosure, or processing of GMAC Personal Data and ensure a level of security appropriate to the risks presented by the processing, including, at a minimum, those measures set forth in Appendix 2 to this DPA;

c. treat GMAC Personal Data with strict confidence and take all reasonable steps to ensure that persons who will Process GMAC Personal Data on its behalf are aware of and comply with the Agreement and this DPA and are under a duty of confidentiality with respect to GMAC Personal Data that is no less restrictive than the duties set forth herein; and

d. not "sell" or "share" GMAC Personal Data, as those terms are defined in applicable Data Protection Laws, or except as expressly permitted under the Agreement, otherwise transfer GMAC Personal Data to any third parties except Processors who are subject to written contracts that guarantee at least the same level of data protection as provided for herein.

3. Security Incidents. The Recipient shall promptly, and no later than twenty-four (24) hours from discovery, notify GMAC at privacy@gmac.com of any actual or reasonably suspected Security

Incident impacting GMAC Personal Data, and promptly provide GMAC with information on the nature of the Security Incident, the GMAC Personal Data affected, and the Recipient's response to and mitigation of the Security Incident. To the extent required by applicable law, or otherwise advisable as determined by GMAC to prevent harm to affected individuals, the Recipient shall promptly provide notice to the impacted individuals and relevant governmental authorities, in accordance with applicable law. The Recipient shall promptly and fully investigate and remediate any Security Incidents, provide all such information to GMAC as GMAC may reasonably request, and provide appropriate redress to the affected individuals.

4. Third-Party Communications. In the event that the Recipient receives any communication from an individual, regulator, governmental body, or other third party relating to either Party's Processing of GMAC Personal Data, the Recipient shall (unless prohibited by applicable law) promptly notify GMAC of such communication and provide relevant details. The Recipient shall additionally provide all cooperation reasonably requested by GMAC to respond to any such communication received by the Recipient or GMAC, and to fulfill any requests made by any subject of GMAC Personal Data in accordance with applicable Data Protection Laws.

5. Restricted Transfers

5.1. If and to the extent that GMAC's provision of the GMAC Services or provision to the Recipient of GMAC Personal Data involves an EEA Restricted Transfer, GMAC and the Recipient hereby enter into the EU Standard Contractual Clauses, which are incorporated by reference herein. For the purpose of any such EEA Restricted Transfer, the EU Standard Contractual Clauses will be completed as follows:

a. The parties select Module One (Transfer Controller to Controller) and agree that GMAC will act as the "data exporter" and the Recipient will act as the "data importer."

b. For the purpose of Section IV, Clause 17, the parties select Option 2. Where the laws of that EU Member State do not allow for third-party beneficiary rights, the Parties agree that the Clauses shall be governed by the law of Ireland.

c. For the purpose of Section IV, Clause 18, the Parties agree that disputes arising from the Standard Contractual Clauses shall be resolved by the courts in Ireland.

d. Annex I is deemed to be completed with the details set out in Appendix 1 to this DPA.

e. Annex II (Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data) is deemed to be completed with the details set out in Appendix 2 to this DPA.

f. If and to the extent that an EEA Restricted Transfer involves Personal Data originating from Switzerland and is subject to the Swiss Federal Act on Data Protection of 19 June 1992 (the "**FADP**"), the EU Standard Contractual Clauses are deemed to be supplemented with an additional annex that provides as follows: (i) for purposes of Clause 13 and Annex I.C of the EU Standard Contractual Clauses, the competent Supervisory Authority is the Swiss Federal Data Protection and Information Commissioner; (ii) the term "member state" as used in the EU Standard

Contractual Clauses must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18.c; and (iii) references in the EU Standard Contractual Clauses to the GDPR should be understood as references to the FADP.

5.2. If and to the extent that GMAC's provision of the GMAC Services or provision to the Recipient of GMAC Personal Data involves a UK Restricted Transfer, GMAC and the Recipient hereby enter into the EU Standard Contractual Clauses and the UK Addendum, which are incorporated by reference herein. For the purpose of any such UK Restricted Transfer, the UK Addendum will be completed as follows:

a. Table 1 of the UK Addendum is deemed to be completed with the Parties' details and contact information as set forth in Appendix 1 to this DPA.

b. For the purposes of Table 2 of the UK Addendum, the Addendum EU SCCs are the EU Standard Contractual Clauses entered into between GMAC and the Recipient under Section 5.1 of this DPA.

c. For the purposes of Table 3 of the UK Addendum, the Appendix Information is as set forth in Sections 5.1.d and 5.1.e of this DPA.

d. For the purposes of Table 4 of the UK Addendum, the Parties select "Exporter."

6. Processing of De-Identified Data. If and to the extent GMAC provides or makes available to the Recipient any De-Identified Data in connection with the GMAC Services, the Recipient shall (a) take reasonable measures to ensure that De-Identified Data cannot be associated with a natural person; (b) Process De-Identified Data only in a de-identified fashion; (c) not attempt to re-identify De-Identified Data; (d) contractually obligate any recipients of De-Identified Data to comply with this Section 6; and (e) publicly commit to complying with the requirements of this Section 6, such as through a prominent disclosure in its publicly-posted privacy policy, on its website, or similar means. The Recipient acknowledges and agrees that GMAC can exercise reasonable oversight to monitor the Recipient's compliance with this Section 6.

7. Indemnification. To the extent permitted by applicable law and without waiving sovereign immunity (as applicable), the Recipient shall indemnify, defend, and hold harmless GMAC from and against any and all losses, damages, liabilities, and costs (including reasonable attorneys' fees) incurred by GMAC in connection with any claims, suits, actions, or other proceedings asserted by a third party related to any failure by the Recipient to comply with its obligations under this DPA.

8. Termination. GMAC may terminate any contract or engagement between the Parties, including, without limitation, the Agreement, in the event of: (a) a Security Incident that GMAC determines is likely to have a substantial adverse impact on GMAC's relationship with candidates or customers or may otherwise substantially harm its reputation; or (b) a violation of this DPA by the Recipient. This Section in no way limits any termination rights provided under the Agreement.

9. Miscellaneous

9.1. If there is any conflict between this DPA and any Agreement, the terms of this DPA will control.

9.2. This DPA will be effective as of the effective date of the Agreement and will remain in effect for so long as the Agreement remains in effect. Any rights, obligations, or required performance of the Parties in this DPA which by their express terms or nature and context are intended to survive termination or expiration of this DPA will survive any such termination or expiration.

9.3. No amendment to or modification of this DPA is effective unless it is in writing and signed by an authorized representative of each Party. No waiver by any Party of any of the provisions hereof will be effective unless explicitly set forth in writing and signed by the Party so waiving.

9.4. Except as otherwise expressly set forth in the EU Standard Contractual Clauses or the UK Addendum, this DPA and any action related thereto will be governed by, construed, and interpreted in accordance with the law governing the Agreement (if applicable), and any dispute arising under this DPA shall be subject to any applicable jurisdiction and venue selection provisions set forth in the Agreement.

9.5. If any provision of this DPA is held to be invalid or unenforceable by a court of competent jurisdiction, then: (a) such invalidity or unenforceability will not affect the other provisions of this DPA; and (b) such invalid or unenforceable provision will be reformed as necessary to make it valid and enforceable in a manner that most closely approximates the original intent of such provision.

APPENDIX 1

Details of the Processing

A. List of Parties

Data Exporter(s):

Name: Graduate Management Admission Council

Address: 11921 Freedom Drive, Suite 300, Reston, Virginia 20190, USA

Contact person's name, position, and contact details: Jack McCann, Senior Manager, Data Privacy, privacy@gmac.com

Data protection officer's (if any) name, position, and contact details: Jennifer Gorman, VP, Legal, privacy@gmac.com

EU representative's (if any) name, position, and contact details: Bird & Bird GDPR Representative Services SRL, Avenue Louise 23, 1050, Bruxelles, Belgium, EURepresentative.GMAC@twobirds.com, Key Contact: Vincent Rezzouk-Hammachi

Activities relevant to the data transferred: Provision of the GMAC Services to the Recipient pursuant to the Agreement.

Signature and date: By entering into the Agreement and the DPA, GMAC is deemed to have signed this Appendix 1.

Role: Controller

Data Importer:

Name: The Recipient, as identified in the Agreement

Contact details: The contact details for the Recipient as set out in the Agreement or in GMAC's client records for the applicable GMAC Services received by the Recipient

Activities relevant to the data transferred: Receipt of the GMAC Services from GMAC pursuant to the Agreement.

Signature and date: By entering into the Agreement and the DPA, the Recipient is deemed to have signed this Appendix 1.

Role: Controller

B. Description of Transfer

Categories of data subjects whose personal data is transferred

Prospective graduate business or graduate management education students who have agreed to the sharing of their Personal Data through the GMAC Services.

Categories of personal data transferred

First name; last name; email address; phone number; date of birth; gender; age; country of citizenship; location/region of citizenship; country/region, city, and zip/postal code of residence; languages spoken; online identifiers, such as device and IP address; LinkedIn URL; educational background, including, but not limited to, highest level of education attained, highest degree completed, major or primary field of study, undergraduate institution, date of graduation, and undergraduate GPA; work experience; military experience; graduate school admissions tests taken; GMAC assessment dates; GMAC assessment score ranges; GMAC assessment score sending destinations; business school journey stage; graduate school plans and preferences, including, but not limited to, preferred degree, intended academic concentration, preferred study location, preferred learning environment, planned date of enrollment, and intended enrollment status; school/program recommendations, preferences, level of commitment, and level of engagement; post-graduate interests; survey results.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Personal data revealing racial or ethnic origin

The Recipient shall only use this data in accordance with the confidentiality and data protection and security measures set forth in the Agreement and the DPA.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Continuous for the term of the Agreement

Nature and Purposes of Processing

GMAC will provide GMAC Personal Data to the Recipient in accordance with and for the purposes set forth in the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

GMAC Personal Data may be retained for the period(s) specified in the Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The Recipient may transfer GMAC Personal Data to Processors for Processing on the Recipient's behalf in accordance with the terms of the Agreement and the DPA.

C. Competent Supervisory Authority

Data exporter is not established in an EEA country, but falls within the territorial scope of the GDPR in accordance with Article 3(2) GDPR and has appointed a representative pursuant to Article 27(1) GDPR.

The competent supervisory authority is the Belgian Data Protection Authority, Belgium.

APPENDIX 2

Mandatory Administrative, Technical, and Physical Measures

The Recipient shall implement, at a minimum, the administrative, technical, and physical measures described below.

1. Access Controls – policies, procedures, and physical and technical controls: (i) to limit physical access to its information systems and the facility or facilities in which they are housed to properly authorized persons; (ii) to ensure that all members of its workforce who require access to GMAC Personal Data have appropriately controlled access, and to prevent those workforce members and others who should not have access from obtaining access; (iii) to authenticate and permit access only to authorized individuals and to prevent members of its workforce from providing GMAC Personal Data or information relating thereto to unauthorized individuals; and (iv) to encrypt and decrypt GMAC Personal Data where appropriate.

2. Security Awareness and Training – a security awareness and training program for all members of the Recipient's workforce (including, without limitation, management), which includes, without limitation, training on how to implement and comply with the Recipient's written security program that includes appropriate administrative, technical, and physical safeguards designed to ensure the ongoing confidentiality, availability, integrity, security, and resilience of Processing of Personal Data ("**Security Program**").

3. Security Incident Procedures – policies and procedures to detect, respond to, and otherwise address Security Incidents, including, without limitation, procedures to monitor systems and to detect actual and attempted attacks on or intrusions into GMAC Personal Data or information systems relating thereto, and procedures to identify and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, and document Security Incidents and their outcomes.

4. Contingency Planning – policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages GMAC Personal Data or systems that contain GMAC Personal Data, including, without limitation, a data backup plan and a disaster recovery plan.

5. Device and Media Controls – policies and procedures that govern the receipt and removal of hardware and electronic media that contain GMAC Personal Data into and out of a the Recipient facility, and the movement of these items within a the Recipient facility, including, without limitation, policies and procedures to address the final disposition of GMAC Personal Data, and/or the hardware or electronic media on which it is stored, and procedures for removal of GMAC Personal Data from electronic media before the media are made available for re-use.

6. Audit Controls – hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including, without limitation, appropriate logs and reports concerning these security requirements and compliance therewith.

7. Data Integrity – policies and procedures to ensure the confidentiality, integrity, and availability of GMAC Personal Data and protect it from disclosure, improper alteration, or destruction.

8. Storage and Transmission Security – technical security measures to guard against unauthorized access to GMAC Personal Data that is being transmitted over an electronic communications network, including, without limitation, a mechanism to encrypt GMAC Personal Data in electronic form while in transit and in storage on networks or systems to which unauthorized individuals may have access.

9. Assigned Security Responsibility – The Recipient shall designate a security official responsible for the development, implementation, and maintenance of its Security Program. The Recipient shall, upon GMAC's request, inform GMAC as to the person responsible for security.

10. Testing – The Recipient shall regularly test and monitor the effectiveness of its Security Program. The Recipient will periodically identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the GMAC Personal Data and ensure that these risks are addressed. Without limiting the foregoing, the Recipient shall conduct penetration testing and vulnerability scans of all computer systems used to Process GMAC Personal Data and promptly implement, at the Recipient's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing. the Recipient will also monitor its workforce for compliance with these requirements. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the Security Program.

11. Adjust the Program – The Recipient shall monitor, evaluate, and adjust, as appropriate, its Security Program in light of any relevant changes in technology or industry security standards, the sensitivity of the GMAC Personal Data, internal or external threats to the Recipient or the GMAC Personal Data, and the Recipient's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.