VERACROSS DATA PROCESSING AGREEMENT

Version 1.6, effective November 2026

This agreement is dated as of the date of its signature by the last party signing (the **Effective Date**).

BACKGROUND

1. The Company and the Customer entered into a Company Software and Service Agreement or other form of agreement (**Agreement**) that may require Company to process Personal Data on behalf of the Customer.
2. This Data Processing Agreement (**DPA**) sets out the additional terms, requirements and conditions on which Company will process Customer Personal Information when providing services under the Agreement.

Customer enters into this DPA on its own behalf and on behalf of its Affiliates, if and to the extent Company Processes Customer Personal Information for which such Affiliates qualify as Controller.

In consideration of the Parties' mutual rights and obligations set out in the Agreement and this DPA, the Parties agree as follows:

1. DEFINITIONS

1.1. "**Affiliate**" shall mean, as to any entity, any other entity that, directly or indirectly, controls, is controlled by or is under common control with such entity.

1.2. "**ANPD Standard Contractual Clauses" means** the standard contractual clauses for international transfers of personal data set out in Annex II to the ANPD Regulation.

1.3. "**Australian Data Protection Law" means** the *Privacy Act 1988 (Cth)* and the Australian Privacy Principles (APPs), as well as, if and to the extent applicable, Australian health data legislation, including without limitation, the *My Health Records Act 2012 (Cth)*, the *Health Records and Information Privacy Act 2002 (NSW)* and its Health Privacy Principles, the *Health Records Act 2001 (Vic)* and its Health Privacy Principles, the *Health Records (Privacy and Access) Act 1997 (ACT)* and its privacy principles, and the *Information Privacy Act 2009 (Qld)* and its privacy principles.

1.4. "**Brazilian Data Protection Law" means** Brazil's General Data Protection Law (Lei Geral de Proteção de Dados Pessoais, Law No. 13,709 of August 14, 2018) (LGPD), as amended, and the regulations issued under it by the Brazilian National Data Protection Authority (ANPD), including the Regulation on International Data Transfers approved by Resolution CD/ANPD No. 19 of August 23, 2024 (ANPD Regulation).

1.5. **"CCPA"** means the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), the CCPA Regulations (Cal. Code Regs. tit. 11, §§ 999.300 to 999.337), as amended by the California Privacy Rights Act of 2020 (CPRA), and any related regulations or guidance provided by the California Attorney General. Terms defined in the CCPA, including "business", "business purposes", "consumer", "personal information", "sale", "sell", "selling", and "service provider" carry the same meaning in this DPA.

1.6. "**Canadian Data Protection Law**" means, as applicable, the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, the *Personal Information Protection Act*, R.S.A. 2003, c. P-6.5, the *Personal Information Protection Act*, R.S.B.C. 2003, c. 63 and *an Act respecting the protection of personal information in the private sector*, CQLR, c. P-39.1, as amended by Law 25, An Act to modernize legislative provisions as regards the protection of personal information.

1.7. "**Chinese Data Protection Law**" means the Cybersecurity Law of the PRC 2016 and the Personal Information Protection Law of the PRC 2021.

1.8. "**Commissioner**" means, in the UK, the UK Information Commissioner (see Article 4(A3), UK GDPR and section 114, DPA 2018), in Australia, the Office of the Australian Information Commissioner, the Office of the Information Commissioner Queensland, or the Office of the Victorian Information Commissioner (as applicable), in New Zealand, the Privacy Commissioner holding office under the Privacy Act 2020, and, in Singapore, the Commissioner for Personal Data Protection appointed under section 8(1)(a) of the PDPA.

1.9. "**Company Security Standards**" means the security standards described in Section 3.1.

1.10. "**Controller**" or "PI Processor" shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

1.11. "**Customer Personal Information**" shall mean, as further described in Annexes I-A and I-B (as applicable), the Personal Data which Company is Processing as Processor on behalf of Customer in order to provide the Services.

1.12. "**Data Protection Laws**" shall mean all data protection and privacy laws applicable to the respective party in its role in the processing of Personal Data under the Agreement, including, where applicable based on the location of the data subject, the Australian Data Protection Law, the New Zealand Privacy Act 2020 (NZ) and the associated Information Privacy Principles (IPPs), the PDPA, the Chinese Data Protection Law, the EU Data Protection Law, UK Data Protection Law, the Canadian Data Protection Law, the Brazilian Data Protection Law, the Mexican Data Protection Law and/or the U.S. Data Protection Law.

1.13. "**EU Data Protection Law**" shall mean all applicable privacy and data protection laws in the EU and Switzerland, including, without limitation, (i) the GDPR, and any equivalent or replacement law in any Member State and all and any regulations made under those acts or regulations; (ii) the Privacy and Electronic Communications Directive (*2002/58/EC*) ("ePrivacy Directive") and any replacement law or regulation in the EU, and any applicable national implementing laws, regulations and secondary legislation in any Member State, in relation thereto; (iii) the Swiss Federal Data Protection Act of 19 June 1992, as amended by the new Swiss Data Protection Act (the "revFADP"), as of September 1st, 2023; in each of (i), (ii) and (iii), as may be amended, superseded or replaced; (iv) the guidelines, recommendations, best practice opinions, directions, decisions, and codes of conduct issued, adopted or approved by the European Commission, the European Data Protection Board, the Swiss Federal Data Protection and Information Commissioner, and/or any supervisory authority or data protection authority from time to time in relation to the GDPR, the ePrivacy Directive, the revFADP and any other applicable privacy and data protection laws; and (v) any judgments of any relevant court of law relating to the processing of personal data, data privacy, and data security.

1.14. "**EU Standard Contractual Clauses**" shall mean the EU Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries set forth in the Commission Decision 2021/914 of 4 June 2021, as well as under any new laws, rules, regulations, and/or contracts that that replace, supersede, or are required to be implemented in connection with the Standard Contractual Clauses.

1.15. "**GDPR**" means the EU General Data Protection Regulation ((EU) 2016/679)) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.16. "**Legitimate Business Purposes**" means the exhaustive list of specific purposes for which Company is allowed to Process the Customer Personal Information as Controller as specified in Section 2.9.

1.17. "**Member State**" shall mean a country that is a member of the European Union or of the European Economic Area.

1.18. "**Mexican Data Protection Law" means** Mexico's Federal Law on the Protection of Personal Data Held by

Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares), published in the Official Gazette of the Federation on March 20, 2025, as amended, and the regulations issued under it.

1.19. "**PDPA**" means Singapore's Personal Data Protection Act of 2012 and Personal Data Protection (Amendment) Act 2020.

1.20. "**Personal Data**" or **"Personal Information"** shall mean any information relating to an identified or identifiable natural person ("**Data Subject**") or a household (as applicable), which information is subject to Data Protection Laws; 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 such as an IP or MAC Address or Mobile ID, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1.21. "**Personal Data Breach**" shall mean a suspected or actual breach of the Company Security Standards leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Customer Personal Information transmitted, stored or otherwise Processed.

1.22. "**Process**" or "**Processing**" shall mean the collection, recording, organization, alteration, use, access, disclosure, copying, transfer, storage, deletion, combination, destruction, disposal or other use of Customer Personal Information by Company on behalf of Customer.

1.23. "**Processor**" or "**Data Intermediary**" (as these terms are defined in Data Protection Laws) shall mean a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller or another organization, as applicable.

1.24. "**Provisions on the Standard Contract for Exports of Personal Information 2023**" means the Cyberspace Administration of China (CAC)'s 2023 Standard Contract Provisions for the outbound transfer of personal information to a location outside the PRC, available here

1.25. "**Services**" shall mean the services provided by Company as described in the Agreement.

1.26. "**Sub-processor**" means any subcontractor engaged by Company for the Processing of Customer Personal Information in accordance with Section 8.1.

1.27. "**Supervisory Authority**" shall mean the relevant privacy regulator in the territories where the parties to this agreement are established (other than the Commissioner), including without limitation the Cyber Administration of China, the California Privacy Protection Agency, the ANPD, the Mexican Secretariat of Anti-Corruption and Good Governance (Secretaría Anticorrupción y Buen Gobierno), and any other U.S. or Canadian federal, state, provincial or EU national independent public authority responsible for data protection matters and which is established pursuant to Data Protection Laws.

1.28. "**Transfer**" shall mean the access by, transfer or delivery to, or disclosure of Personal Data to a person, entity or system located in a country or jurisdiction other than the country or jurisdiction where the Personal Data originated from.

1.29. "**UK Data Protection Law**" shall mean all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (**DPA 2018**); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data (including, without limitation, the privacy of electronic communications); and the guidance and codes of practice issued by the Commissioner or other relevant regulatory authority and which are applicable to a party.

1.30. "**UK GDPR**" shall have the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the DPA 2018.

1.31. "**UK International Data Transfer Agreement**" (IDTA) shall mean the standalone international data transfer agreement or the international data transfer addendum to the EU Standard Contractual Clauses (as

applicable) issued by the UK Information Commissioner's Office under Section 119A of the DPA 2018 and which came into force on 21 March 2022, in replacement of the UK standard contractual clauses for transfers of UK personal data to a location outside of the UK.

1.32. **"U.S. Data Protection Law"** shall mean all applicable data protection and privacy legislation in force from time to time in the U.S., including without limitation, the CCPA, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Nevada online privacy law, the Texas Data Privacy and Security Act, the Utah Consumer Privacy Act, the Virginia Consumer Data Protection Act, the Delaware Personal data Privacy Act, the Florida Digital Bill of Rights, the Indiana Consumer Data Protection Act, the Iowa Consumer Data Protection Act, the Kentucky Consumer Data Protection Act, the Maryland Online Data Privacy Act, the Montana Consumer Data Privacy Act, the Nebraska Data Privacy Act, the New Hampshire Consumer Data Privacy Act, the New Jersey Consumer Data Privacy Act, the Oregon Consumer Privacy Act, the Rhode Island Data Privacy Act, the Tennessee Information Protection Act, and U.S. Student Privacy Laws.

1.33. "**U.S. Student Privacy Laws**" shall mean all applicable laws governing student privacy, including federal statutes such as the Family Educational Rights and Privacy Act (FERPA), the Protection of Pupil Rights Amendment (PPRA), and the Children's Online Privacy Protection Act (COPPA); and state statutes, which may reinforce or provide greater protections than FERPA and other federal laws.

2. DATA PROCESSING

2.1. This DPA applies if and to the extent Company is Processing Customer Personal Information. In this context, Company will act as a "Processor" or "Service Provider" to the Customer, who may act as "Controller" or "Business", or "Processor" or "Service Provider" with respect to Customer Personal Information.

2.2. Annex I (Processing Details) sets out:

2.2.1. the nature, purposes, and subject matter of the Processing;

2.2.2. the duration of the Processing;

2.2.3. the categories of Data Subjects; and

2.2.4. the types of Customer Personal Information.

2.3. Company will Process the Customer Personal Information for the sole purpose of providing the Services according to Customer's written instructions. For Personal Information that is subject to the CCPA, Company acknowledges that it is prohibited from: (i) selling or sharing such Personal Information; (ii) retaining, using, or disclosing such Personal Information for a commercial purpose other than providing the Services or as otherwise permitted by the CCPA; (iii) retaining, using, or disclosing such Personal Information outside of the Agreement or other direct business relationship between Company and Customer; and (iv) unless used for a business purpose that does not involve cross-context behavioural advertising and is permitted under eventual CPRA regulations, combining the Personal Information with personal information that Company (a) receives from, or on behalf of, another person or persons; or (b) collects from its own consumer interaction.

2.4. The Parties agree that the Agreement and this DPA constitute Customer's complete and final documented instructions to Company in relation to the Processing of Customer Personal Information. Additional instructions outside the scope of the Agreement or this DPA (if any) require prior written agreement between Company and Customer, including agreement on any additional fees payable by Customer for carrying out such instructions. Customer shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Customer Personal Information, and that the Processing of the Customer Personal Information in accordance with Customer's instructions will not cause Company to be in breach of the Data Protection Laws.

2.5. Company will not access or use the Customer Personal Information, except as necessary to maintain or provide the Services, or as necessary to comply with the law or a binding order of a governmental body.

2.6. Company will reasonably assist Customer, at no additional cost to the Customer, with meeting

Customer's compliance obligations under the Data Protection Laws, taking into account the nature of Company's processing and the information available to Company, including in relation to data protection impact assessments and reporting to and consulting with Supervisory Authorities under applicable Data Protection Laws.

2.7. Customer agrees that (i) it will comply with its obligations under Data Protection Laws (if and to the extent applicable based on the location of the data subject) in respect of its Processing of the Customer Personal Information, including any obligations specific to its role as a Controller/PI Processor/Business and/or Processor/Service Provider/Data Intermediary (as applicable, based on the applicable Data Protection Laws); or as an educational institution subject to U.S. Student Privacy Laws or other applicable Data Protection Laws governing the collection and processing of student data; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under applicable Data Protection Laws for Company to Process the Customer Personal Information, including Processing of EU Personal Data in a location outside of the EEA or the Personal Information of Australian, Brazilian, Canadian, Chinese, Mexican, or Singaporean residents outside Australia, Brazil, Canada, China, Mexico, or Singapore (as and to the extent applicable), as required to provide the Services pursuant to the Agreement and this DPA. If Customer is itself a Processor/Service Provider/Data Intermediary (as applicable, based on applicable Data Protection Laws), Customer warrants to Company that Customer's instructions and actions with respect to that Customer Personal Information, including its appointment of Company as another Processor/Service Provider/Data Intermediary, have been authorized by the relevant Controller/PI Processor/Business or other organization under applicable Data Protection Laws.

2.8. In particular in relation to any Sensitive Information, as this term is defined under Australian Data Protection Law, Customer warrants that it:

2.8.1. will not provide any Sensitive Information to Company unless that information is necessary for Customer to perform its obligations;

2.8.2. has:

(i) made all necessary notifications required by APP 5, on behalf of itself and Company to;

and

(ii) obtained consent as required by APP 8.2(b), on behalf of itself and Company from,

the individuals whose Sensitive Information it is disclosing to Company in the course of this DPA to enable Company to lawfully Process the Sensitive Information and perform its obligations in accordance with this DPA.

2.9. Company may Process some Customer Personal Information for its own Legitimate Business Purposes, as an independent Controller, solely when the Processing is strictly necessary and proportionate, and if the Processing is for one of the following exhaustive list of purposes: (a) directly identifiable data (job title, name, email address, phone number, technical usage data) may be Processed for: (i) billing, account, and Customer relationship management (marketing communication with procurement/sales employees of Company), and related Customer correspondence (mailings about for example necessary updates); (ii) complying with and resolving legal obligations, including responding to Data Subject Requests for Personal Data processed by Company as data Controller (for example Website data), tax requirements, agreements and disputes; (iii) abuse detection prevention and protection, virus scanning and scanning to detect violations of terms of service (such as copyright infringement, SPAM, and actions not permitted under Company's Terms of Use); (b) pseudonymized and/or aggregated data (Company will pseudonymize and/or aggregate as much as possible and pseudonymized and/or aggregated data will not be processed on a per-Customer level); for: (i) improving and optimizing the performance and core functionalities of accessibility, privacy, security, and the IT infrastructure efficiency of the Services and Website; (ii) internal reporting, financial reporting, revenue planning, capacity planning, and forecast modeling (including

product strategy); (iii) receiving and using Feedback for Company's overall service improvement. When acting as an independent Controller/PI Processor, Company will not Process Customer Personal Information for any purposes other than the Legitimate Business Purposes listed above, or as provided in Section 2.10.

2.10. Company may (a) derive and compile from the provision of the Services certain de-identified, aggregate and/or analytical data, which shall not contain any Customer-specific or any individually identifying information (Generic Data), and (b) use Generic Data for Company's own purposes and without restriction, including but not limited to for use in conjunction with data from other sources to improve Company's products and services and create new data models and products.

3. TECHNICAL AND ORGANIZATIONAL MEASURES

3.1. Company will implement and maintain technical and organizational measures to ensure a level of security appropriate to the risk as described in our Trust Center. Company also uses Salesforce (SFDC) as a third-party data processor. SFDC requires that we refer in this DPA to their technical and organizational measures as found in SFDC's Security, Privacy and Architecture Documentation accessible via SFDC's Trust and Compliance webpage (also accessible here under SFDC's Trust and Compliance Documentation, or as otherwise made available by SFDC).

3.2. Customer is responsible for reviewing the information made available by Company relating to data security and making an independent determination as to whether the technical and organizational measures implemented by Company and SFDC meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Company Security Standards and SFDC's technical and organizational measures are subject to technical progress and further development and that Company and SFDC may update or modify the Company Security Standards and/or SFDC technical and organizational measures from time to time provided that such updates and modifications do not result in a material degradation of the overall security of the Services provided to Customer under the Agreement.

3.3. Customer agrees that, without prejudice to Company's obligations under Section 3.1: (a) Customer is responsible for its use of the Services, including making appropriate use of the Services to ensure a level of security appropriate to the risk in respect of the Customer Personal Information, securing its account authentication credentials, managing its data back-up strategies, and protecting the security of the Customer Personal Information when in transit to and from the Services and taking any appropriate steps to securely encrypt or backup any Customer Personal Information uploaded to the Services; and (b) Company has no obligation to protect the Customer Personal Information that Customer elects to store or transfer outside of Company's and its Sub-processors' systems (for example, offline or on premise storage).

4. DATA SUBJECT RIGHTS AND REQUESTS

4.1. Company shall, to the extent permitted by applicable Data Protection Laws, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject when acting as a Processor, such as a Data Subject's right of access, right to rectification, restrict the processing, erasure ("right to be forgotten"), data portability, object to the processing or his/her rights not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Company shall not respond to a Data Subject Request itself, except that Customer authorizes Company to redirect the Data Subject Request as necessary to allow Customer to respond directly. Taking into account the nature of the processing, Company shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Company shall, upon Customer's request, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Company is legally permitted to do so and the response to such Data Subject request is required under applicable Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any

costs arising from Company's provision of such assistance.

4.2. Customer agrees that, without prejudice to the Company's obligations under Section 4.1 above, Customer is solely responsible for dealing with Data Subject requests.

4.3. If a law enforcement agency sends Company a demand for Customer Personal Information (e.g., a subpoena or court order), Company will redirect the law enforcement agency to request that data directly from Customer. As part of this effort, Company may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Information to a law enforcement agency, then Company will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent Company is legally permitted to do so.

4.4. Customer acknowledges that Company is required under EU and UK Data Protection Law to: (a) collect and maintain written records of certain information, including the name and contact details of each Processor and/or Controller on behalf of which Company is acting and, where applicable, of such Processor's or Controller's local representative and data protection officer, and (b) make such information available to the Supervisory Authorities. Accordingly, if EU and UK Data Protection Law applies to the Processing of the Customer Personal Information, Customer will, where requested, provide such information to Company via the Services or other means provided by Company, and will ensure that all information provided is kept accurate and up-to-date.

5. CONFIDENTIALITY

5.1. Without prejudice to any existing contractual arrangements between the Parties, Company shall treat all Customer Personal Information as strictly confidential and shall inform all its employees, agents and/or approved Sub-processors engaged in Processing the Customer Personal Information of the confidential nature of the data. Company shall ensure that all such persons or parties have signed an appropriate confidentiality agreement, are otherwise bound to a duty of confidentiality, or are under an appropriate statutory obligation of confidentiality.

5.2. Company will not disclose the Customer Personal Information to any third party, unless authorized by Customer or required by mandatory law. If a government or Supervisory Authority demands access to Customer Personal Information, Company will notify Customer prior to disclosure unless prohibited by law.

6. INFORMATION AND AUDIT

6.1. Customer acknowledges that Company is regularly audited by independent third-party auditors and/or internal auditors against the standards specified in the Company Security Standards, as described in Section 3.1. Upon request, Company shall supply (on a confidential basis) a summary copy of its audit report(s) to Customer, so that Customer can verify the Company's compliance with the audit standards against which it has been assessed, and this DPA. If the Agreement does not include a provision protecting the Company's confidential information, then any audit report(s) will be made available to Customer subject to a mutually agreed upon non-disclosure agreement covering those reports.

6.2. Company shall also provide written responses (on a confidential basis) to all reasonable requests for information made by Customer related to its Processing of the Customer Personal Information, including responses to information security questionnaires that are necessary to confirm the Company's compliance with this DPA, provided that Customer shall not exercise this right more than once per year.

6.3. Customer agrees to exercise any right it may have to conduct an audit or inspection of the Company's technical and organization measures, including under the EU 2021 Standard Contractual Clauses and/or UK International Data Transfer Agreement if they apply, by instructing Company to carry out such audit.

7. RETURNING OR DELETING CUSTOMER PERSONAL INFORMATION

7.1. Upon termination or expiration of the Agreement, or anytime upon Customer's written request, Company shall promptly make available for download and/or delete all copies of the Customer Personal Information which Company Processes as a Processor; provided, however, that Company shall not be required to return or delete Customer Personal Information to the extent Company is required by applicable law or order of a governmental or regulatory body to retain all or some of the Customer Personal Information.

7.2. Customer acknowledges and agrees that SFDC will return Customer Personal Information to Company and, to the extent allowed by applicable law, will delete Customer Personal Information in accordance with the procedures and timeframes specified in SFDC's Security, Privacy and Architecture Documentation.

7.3. For purposes of clarification, the above obligations shall not apply to (i) Customer Personal Information for which Company acts as a Controller or PI Processor, as provided in Section 2.9; or (ii) any Generic Data, as provided in Section 2.10.

8. SUB-PROCESSORS

8.1. Customer acknowledges and agrees that:

8.1.1. Company may engage Sub-processors to Process Customer Personal Information on Customer's behalf. Customer hereby consents to Company continuing to use any of Company's Affiliates and all Sub-processors already engaged by Company as at the date of this DPA (a full list is available here), including, in the case of Salesforce, their Affiliates and their respective sub-processors.

8.1.2. SFDC's Affiliates may be retained as Sub-processors; and SFDC and SFDC's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. The current list of Sub-processors engaged by SFDC and its Affiliates in Processing Customer Personal Information for the performance in connection with the performance of the Services, including a description of their Processing activities and countries of location, is listed under the Infrastructure and Sub-processor Documentation which can be found on SFDC's Trust and Compliance webpage (also accessible here under SFDC's Trust and Compliance Documentation). Customer hereby consents to these Sub-processors, their locations and Processing activities as it pertains to the Customer Personal Information. Customer shall promptly take any reasonable action required or appropriate to facilitate or support any transfer of Customer Personal Information to approved Sub-processors (e.g., updating registrations with Supervisory Authorities).

8.1.3. Company shall notify Customer of any new Sub-processor Company wishes to appoint to carry out Processing activities on behalf of Customer. If, within two (2) weeks of receipt of any such notice, Customer notifies Company in writing of any objections to the proposed appointment for legitimate reasons, Company shall work with Customer in good faith to take reasonable measures to address the objections raised by Customer, and where such measures cannot be agreed within three (3) weeks from the Company's receipt of Customer's notice, Customer may by written notice to Company with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Sub-processor. "Legitimate reasons" shall be deemed given if there is an indication based on objective facts which reasonably support the assumption that the engagement of the sub-processor would breach applicable law or this DPA.

8.1.4. Where Company engages a Sub-processor to carry out specific Processing activities on behalf of Customer, Company shall enter into a written agreement with the Sub-processor which includes terms which offer the same level of protection for the Customer Personal Information as those set out in this DPA. If and to the extent that the Customer Personal Information processed by the Sub-processors qualifies as Personal Information under the CCPA, any such Sub-processors used must qualify as a service provider under the CCPA and Company cannot make any disclosures to the Sub-processor that the CCPA would treat as a sale.

8.1.5. Notwithstanding any approval by Customer within the meaning of Sections 8.1.1 and/or 8.1.2, Company shall remain fully liable vis-à-vis Customer for the performance of any such Sub-processor that fails to fulfil its data protection obligations under this DPA and/or any applicable Data Protection Laws.

9. TRANSFERS OF PERSONAL INFORMATION

9.1. Company and its subsidiaries participate in and have certified their compliance with the EU-U.S. Data Privacy Framework (DPF) Program, the Swiss-U.S. Privacy Framework (DPF) Program, and the UK Extension thereto, as such programs are administered by the US Department of Commerce. Company and its subsidiaries are committed to subjecting all Customer Personal Information received from European Union (EU) member countries, the UK, and Switzerland, respectively, in reliance on each DPF Program, to the Program's applicable Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement, and Liability. To learn more about the DPF Programs, and to view our certification, visit the U.S. Department of Commerce's DPF Program Participants List at https://www.dataprivacyframework.gov/s/participant-search.

9.2. Company is responsible for the Processing of Personal Information it receives, under each DPF Program, and subsequently transfers to a third party acting as an agent on its behalf. Company complies with the DPF Principles for all onward transfers of Customer Personal Information from the EU, UK and Switzerland, including the onward transfer liability provisions.

9.3. With respect to Customer Personal Information received or transferred pursuant to the DPF Programs, Company is subject to the investigatory and enforcement authority of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

9.4. Following the invalidation of the EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield Frameworks as lawful mechanisms for transferring EU or Swiss personal information to the U.S., as a result of the Court of Justice of the European Union's "Schrems II" ruling of July 16, 2020, Company is also using the Model Contract terms issued by the European Commission in the form that can be accessed here in connection with any transfer to the U.S. of Customer Personal Information from the EU and/or Switzerland for which Company acts as a Processor.

9.5. To the extent that Company Processes as a Processor any Customer Personal Information that originates from the United Kingdom in a country that has not been designated by the UK Secretary of State as providing an adequate level of protection for Personal Data, Company shall also enter into a UK IDTA with Customer in the form that can be accessed here. Where applicable, the signed UK IDTA shall form an integral part of this DPA as if fully set forth herein. The information required by Appendix 1 and Appendix 2 to the UK IDTA is set forth in Annex I-A hereto.

9.6. To the extent that Customer or Company are relying on a specific statutory mechanism to normalize international Personal Data Transfers that is subsequently modified, revoked, or held in a court of competent jurisdiction to be invalid, Customer and Company agree to cooperate in good faith to promptly terminate the Transfer or to pursue a suitable alternative mechanism that can lawfully support the Transfer.

9.7. For the purposes of the EU Standard Contractual Clauses to be entered into between the parties, the following shall apply:

9.7.1. The list of parties and description of the transfer in Annex I of the Clauses shall be as described in Annex I to this DPA.

9.7.2. The technical and organizational measures in Annex II of the Clauses shall be as described in Section 3.1.

9.8. To the extent that Company Processes as a Processor any Customer Personal Information that originates from Australia in a country outside Australia, Company will take reasonable steps in accordance with APP 8.1 and state and territorial Australian health data legislation to make sure the overseas recipient will not breach the APPs and applicable state and territorial health data-related privacy principles. In particular, Company shall not transfer any Customer Personal Information to a third party located outside Australia unless the third party:

9.8.1. agrees to comply with the APPs and state and territorial privacy principles in relation to the collection, use, disclosure, storage and destruction or de-identification of Personal Information disclosed to it in the course of this Agreement;

9.8.2. has an established complaint handling process for privacy complaints; and

9.8.3. has a data breach response plan which includes a mechanism for notifying Customer where there are reasonable grounds to suspect a Personal Data Breach and outlines appropriate remedial action (based on the type of Personal Information to be handled under the Agreement).

9.9. To the extent that Company Processes any Customer Personal Information that originates from New Zealand in a country outside New Zealand, Company will take reasonable steps in accordance with IPP 12 to make sure the overseas recipient will not breach the IPPs. In particular, Company shall not transfer any Customer Personal Information that originates from New Zealand to a third party located outside New Zealand unless the overseas recipient agrees to enter into an agreement with Company that provides for comparable safeguards for the personal information to those in the New Zealand Privacy Act, such as the model contract clauses developed by the Office of the Privacy Commissioner of New Zealand.

9.10. To the extent that Company Processes as a Processor any Customer Personal Information that originates from Brazil in a country outside Brazil, Company may enter into the ANPD Standard Contractual Clauses with Customer, with Customer as data exporter and Company as data importer, as directed by the customer. Where applicable, the ANPD Standard Contractual Clauses form an integral part of this DPA and prevail over this DPA to the extent of any conflict.

9.11. Customer Personal Information that originates from Mexico and that Company Processes as a Processor is provided to Company as a remission (remisión) to a processor (encargado) under the Mexican Data Protection Law, and Company will Process it as an encargado in accordance with this DPA.

10. INFORMATION OBLIGATIONS AND PERSONAL DATA BREACH

10.1. If Company becomes aware of a Personal Data Breach that impacts the Processing of the Customer Personal Information, Company will without undue delay: (a) notify Customer of the Personal Data Breach; and (b) take reasonable steps to minimize any damage resulting from the Personal Data Breach.

10.2. To assist Customer in relation to any Personal Data Breach notifications Customer is required to make under the Data Protection Laws, Company will include in the notification under Section 10.1(a) such information about the Personal Data Breach as Company is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to the Company, and any restrictions on disclosing the information, such as confidentiality.

10.3. Customer agrees that:

10.3.1. An unsuccessful Personal Data Breach will not be subject to this Section 10. An unsuccessful Personal Data Breach is one that results in no unauthorized access to Customer Personal Information or to any of the Company's equipment or facilities storing Customer Personal Information, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar events; and

10.3.2. The Company's obligation to report or respond to a Personal Data Breach under this Section 10 is not and will not be construed as an acknowledgment by Company of any fault or liability of

Company with respect to the Personal Data Breach.

10.4. Notification of Personal Data Breaches, if any, will be delivered to one or more of Customer's administrators by any means Company selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the Company's systems, and secure transmission at all times.

10.5. Customer acknowledges that Company will not assess the contents of the Customer Personal Information in order to identify information subject to any specific legal requirements. Customer is solely responsible for complying with the data breach notification obligations applicable to Customer under Data Protection Laws and fulfilling any third-party notification obligations related to any Personal Data Breach.

11. CCPA WARRANTIES

11.1. Company warrants that it has no reason to believe any CCPA requirements or restrictions, if and to the extent applicable, prevent it from providing the Services or otherwise performing its obligations under this DPA. Company will promptly notify Customer of any changes to the CCPA's requirements that may adversely affect its performance under this DPA.

11.2. Both parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing Customer Personal Information.

12. LIABILITY

12.1. The liability of each Party under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Customer agrees that any regulatory penalties incurred by Company in relation to the Customer Personal Information that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA and Data Protection Laws shall count towards and reduce the Company's liability under the Agreement as if it were liability to Customer under the Agreement.

13. GENERAL

13.1. If any provision of this DPA is ineffective or void, this shall not affect the remaining provisions. The parties shall replace the ineffective or void provision with a lawful provision that reflects the business purpose of the ineffective or void provision. In case a necessary provision is missing, the parties shall add an appropriate one in good faith.

13.2. In the event of any inconsistency between the provisions of this DPA and the provisions of the Agreement, the provisions of this DPA shall prevail in respect of the Processing of Customer Personal Information.

13.3. This DPA (insofar as relates to any EU or Swiss Personal Data, if any, being Processed hereunder) and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this DPA, or its subject matter or formation, shall be governed by and construed in accordance with the laws of the Federal Republic of Germany or Switzerland, respectively.

13.4. This DPA (insofar as relates to any UK Personal Data, if any, being Processed hereunder), and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this DPA (only insofar as relates to UK Personal Data being Processed hereunder) or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales.

13.5. This DPA (insofar as relates to any Singaporean Personal Data, if any, being Processed hereunder) and any dispute or claim arising out of or in connection with this DPA shall be governed by and construed in accordance with the laws of Singapore.

13.6. This DPA (insofar as relates to any Australian Personal Data, if any, being Processed hereunder) and all matters arising out of or relating thereto, shall be governed by and construed in accordance with the laws of Queensland, Australia, without giving effect to the conflict of laws provisions thereof to the extent such principles or rules would require or permit the application of the laws of any jurisdiction other than those of Queensland, Australia.

13.7. This DPA (insofar as relates to any New Zealand Personal Data, if any, being Processed hereunder) and all matters arising out of or relating thereto, shall be governed by and construed in accordance with the laws of New Zealand, without giving effect to the conflict of laws provisions thereof to the extent such principles or rules would require or permit the application of the laws of any jurisdiction other than those of New Zealand.

13.8. This DPA (insofar as relates to any other Personal Data, if any, being Processed hereunder) and all matters arising out of or relating to this DPA, whether sounding in contract, tort, or statute, shall be governed by and construed in accordance with the laws of the Commonwealth of Massachusetts, without giving effect to the conflict of laws provisions thereof to the extent such principles or rules would require or permit the application of the laws of any jurisdiction other than those of the Commonwealth of Massachusetts.

13.9. Each Party irrevocably agrees that the courts of the Federal Republic of Germany or of Switzerland (as applicable) shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the processing of any EU or Swiss Personal Data, respectively, under this DPA or its subject matter or formation.

13.10. Each Party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with the processing of any UK Personal Data under this DPA or its subject matter or formation.

13.11. Each Party irrevocably agrees that the courts of Queensland, Australia shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims), arising out of or in connection with this DPA or its subject matter or formation, as regards the Processing of Personal Data relating to Data Subjects based in Australia.

13.12. Each Party irrevocably and unconditionally agrees that it will not commence any action, litigation, or proceeding of any kind whatsoever against the other Party in any way arising from or relating to any Processing of any New Zealand Personal Data under this DPA, in any forum other than the courts of New Zealand. Each Party irrevocably and unconditionally submits to the exclusive jurisdiction of such courts and agrees to bring any such action, litigation, or proceeding only in the courts of New Zealand. Each Party agrees that a final judgment in any such action, litigation, or proceeding is conclusive and may be enforced in other jurisdictions by suit on the judgment or in any other manner provided by law.

13.13. Each Party irrevocably and unconditionally agrees that it will not commence any action, litigation, or proceeding of any kind whatsoever against the other Party in any way arising from or relating to any Processing of U.S. Personal Data under this DPA, including, but not limited to, contract, equity, tort, fraud, and statutory claims, in any forum other than the courts of the Commonwealth of Massachusetts and any appellate court from any thereof. Each Party irrevocably and unconditionally submits to the exclusive jurisdiction of such courts and agrees to bring any such action, litigation, or proceeding only in the courts of the Commonwealth of Massachusetts. Each Party agrees that a final judgment in any such action, litigation, or proceeding is conclusive and may be enforced in other jurisdictions by suit on the judgment or in any other manner provided by law.

Except as otherwise detailed herein, the terms and conditions of the Agreement shall remain unchanged and in full force and effect.

Annex I-A

PROCESSING DETAILS

1. List of Parties

1.1. Customer as the Controller/PI Processor/Data Exporter:

Customer, Customer Subsidiaries, and/or their respective customers are the data controller of certain Customer Personal Data provided to Company to provide the Services. If Customer or Customer Subsidiaries are acting as a Processor they will be deemed a "controller" for purposes of this DPA.

1.2. Company as the Processor/Data Importer:

The entity of the Veracross group named in the applicable Order Form

Contact name, position and contact details:

Data Protection Officer (DPO) privacy@veracross.com

2. Nature of Services provided by Company:
Software development and provision of the School Management Information System and support of customers.

3. Type(s) of Customer Personal Data processed: see our Services Data Processing Table.

4. Special categories of data: see our Services Data Processing Table.

5. Categories of Data Subjects:

Any member of Customer community of individuals accessing the Service including but not limited to: employees, faculty, staff, students, parents, applicants, applicant family members (parents, grandparents, relatives, legal guardians), lawyers, vendors, alumni, and volunteers.

6. Nature of Processing Operations:
The Personal Data processed by Company and/or its Subcontractors will be subject to the processing activities described in the Contract(s) or purchase orders for the services subject to this DPA.

Such processing activities include: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, alignment or combination, restriction, erasure or destruction, and providing support and maintenance to the data exporter, the data exporter's subsidiaries, and/or their respective end users.

Duration of processing: Until the end of the term of the Contract.

7. Data Exports:
Company's legal basis for processing Customer Personal Information outside the EEA in order to comply with cross-border transfer restrictions:

- Standard Contractual Clauses between Customer as "data exporter" and Company as "data importer" (EU data)
- UK International Data Transfer Agreement or Addendum (as applicable) between Customer and Company (UK data).
- EU-U.S. and Swiss-U.S. Data Privacy Frameworks (DPF), and UK Extensions thereto.

Company's legal basis for processing Customer Personal Information outside the PRC in order to comply with cross-border transfer restrictions:

- 2023 Standard Contract Provisions for the outbound transfer of personal information to a location outside the PRC, available here

Company's legal basis for processing Customer Personal Information outside Brazil in order to comply with cross-border transfer restrictions:

- ANPD Standard Contractual Clauses between Customer as data exporter and Company as data importer (Brazilian data).

Annex I-B

PROCESSING DETAILS – CCPA (ONLY COMPLETE TO THE EXTENT APPLICABLE)

Personal Information Categories: This DPA may involve, at the Customer's discretion, the following types of Personal Information, as defined and classified in CCPA Cal. Civ. Code § 1798.140(o), as amended by the CPRA.

Category	**Personal Information**
A. Identifiers.	A real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers.
B. Personal information categories listed in the California Customer Records statute (Cal. Civ. Code § 1798.80(e)).	A name, signature, address, telephone number. Some personal information included in this category may overlap with other categories.
C. Protected classification characteristics under California or federal law.	Age (40 years or older), race, color, ancestry, national origin, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions).
D. Commercial information.	Records of products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.
E. Biometric information.	Physiological, behavioral, and biological characteristics, or activity patterns used to extract a template or other identifier or identifying information.
F. Internet or other similar network activity.	Information on a consumer's interaction with a website, application, or advertisement.
G. Geolocation data.	Physical location.
I. Professional or employment-related information.	Current or past job history or performance evaluations.
J. Non-public education information (per the Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g, 34 C.F.R. Part 99)).	Education records directly related to a student maintained by an educational institution or party acting on its behalf, such as grades, transcripts, class lists, student schedules, student identification codes, student financial information, or student disciplinary records.
K. Inferences drawn from other personal information.	Profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.
L. Sensitive Personal Information	Government identifiers (social security, driver's license, state identification card, or passport number)

	Complete account access credentials (user names, account numbers, or card numbers combined with required access/security code or password) Precise geolocation Racial or ethnic origin Religious or philosophical beliefs Mail, email, or text messages contents not directed to You Unique identifying biometric information Health information

Types of Consumers: Any member of Customer community of individuals accessing the Service including but not limited to employees, faculty, staff, students, parents, applicants, applicant family members (parents, grandparents, relatives, legal guardians), lawyers, vendors, alumni, and volunteers.

Annex I-C

SWISS ADAPTATIONS TO THE EU STANDARD CONTRACTUAL CLAUSES

This Annex I-C forms an integral part of the Data Processing Agreement (the "DPA"). It is automatically incorporated by reference into Section 9 of the DPA and applies to any Processing of Customer Personal Information governed by the revFADP, and to any Transfer of Customer Personal Information from Switzerland to a country that has not been recognized by the Swiss Federal Council as providing an adequate level of protection. No additional signature by Customer or Company is required to give effect to this Annex. Capitalized terms used but not defined in this Annex have the meanings given in the DPA.

1. APPLICATION

1.1. This Annex I-C applies where the EU Standard Contractual Clauses are relied upon as a Transfer mechanism for Customer Personal Information originating from Switzerland, whether in addition to or in place of their application to Customer Personal Information originating from the European Economic Area.

1.2. Where the same Transfer involves Customer Personal Information subject to both the GDPR and the revFADP, the EU Standard Contractual Clauses apply in unmodified form to the portion of the Transfer governed by the GDPR, and the adaptations in Section 2 of this Annex apply to the portion of the Transfer governed by the revFADP. The Supervisory Authority competent for each portion is the authority of the originating jurisdiction.

2. ADAPTATIONS TO THE EU STANDARD CONTRACTUAL CLAUSES

For Transfers of Customer Personal Information governed by the revFADP, the EU Standard Contractual Clauses apply with the following adaptations, consistent with the guidance published by the Swiss Federal Data Protection and Information Commissioner (the "FDPIC"):

2.1. References to "Regulation (EU) 2016/679" or to the "GDPR" within the EU Standard Contractual Clauses shall be read as references to the revFADP, to the extent the Transfer is governed by the revFADP.

2.2. References to "Member State" within the EU Standard Contractual Clauses shall be read as references to Switzerland. Data Subjects in Switzerland shall not be denied the ability to assert their rights in Switzerland on the basis of being located outside a Member State.

2.3. The competent Supervisory Authority for the purposes of Clause 13 and Annex I.C of the EU Standard Contractual Clauses shall be the FDPIC, to the extent the Transfer is governed by the revFADP.

2.4. For the purposes of Clause 17 of the EU Standard Contractual Clauses, the EU Standard Contractual Clauses shall be governed by the laws of Switzerland to the extent the Transfer is governed by the revFADP.

2.5. For the purposes of Clause 18 of the EU Standard Contractual Clauses, any dispute arising from a Transfer governed by the revFADP shall be resolved by the competent courts of Switzerland. Data Subjects retain the right to lodge a complaint with the FDPIC and the right to bring proceedings in the courts of their habitual residence.

3. LEGAL PERSONS

The extension of protection to data about legal persons under prior FDPIC guidance applied only during the transition to the revFADP. From 1 September 2023, the revFADP applies only to natural persons, and no additional protection for legal persons is required under this Annex.

4. INCORPORATION AND ORDER OF PRECEDENCE

4.1. This Annex I-C is incorporated by reference into the DPA and forms an integral part of the DPA. It takes effect

automatically upon the Effective Date of the DPA, or upon the date on which Company first Processes Customer Personal Information governed by the revFADP, whichever is later. No separate execution by Customer or Company is required.

4.2. In the event of any inconsistency between this Annex I-C and any other provision of the DPA, this Annex shall prevail solely with respect to Customer Personal Information governed by the revFADP, and only to the extent of the inconsistency.

4.3. Termination or expiration of the DPA terminates this Annex automatically. Provisions of this Annex that by their nature are intended to survive termination shall survive.