ALVAO SaaS
Data Processing Addendum

July 2026

ALVAO

1 Introduction

1.1 This ALVAO SaaS Data Processing Addendum (the "**DPA**") governs the terms of the processing and security of Customer Personal Data by the Provider as a processor, to the extent that the Provider processes Customer Personal Data on the Customer's behalf when providing the Online Application or Professional Services.

1.2 This DPA applies to the processing of Customer Personal Data within the Online Application or Professional Services, if and to the extent that, in such processing, the Provider acts as a processor under the Data Protection Requirements.

1.3 This DPA does not apply to the processing of personal data where the Provider acts as an independent controller, in particular when processing Service Data or in the course of Limited Business Operations.

1.4 This DPA forms part of the Agreement. In the event of a conflict between this DPA and other parts of the Agreement, this DPA prevails.

1.5 Unless expressly stated otherwise in this DPA, the Terms apply.

1.6 This DPA does not apply to the processing of personal data in environments controlled by the Customer or by third parties selected by the Customer.

2 Definitions

2.1 Capitalized terms used in this DPA but not defined in this DPA have the meaning set out in the "Definitions" article of the Terms.

2.2 The following defined terms are used in this DPA:

"**Customer Data**" means all data, including all text, audio, video, or image files and software, provided to the Provider by the Customer or the Customer's Affiliates, or on their behalf, during the Customer's use of the Online Application. Customer Data does not include Professional Services Data or Service Data.

"**Customer Personal Data**" means Personal Data forming part of Customer Data or Professional Services Data that the Provider processes on the Customer's behalf when providing the Online Application or Professional Services as a processor or subprocessor.

"**Data Protection Requirements**" means the GDPR, the UK GDPR, the Data Protection Act 2018, Local EU/EEA Data Protection Laws, and all applicable laws, regulations, and other legal requirements relating to (a) the protection of privacy and data security and (b) the use, collection, retention, security, disclosure, transfer, disposal, and other forms of processing of any personal data, in each case to the extent they apply to the processing of Personal Data under the Agreement.

"**Deletion**" means the irreversible removal or rendering inaccessible of EDDA and Customer Data from the Provider's systems after termination of the Agreement.

"**EU Customer**" means a customer whose billing address is in the European Union or in the European Economic Area.

"**European Data Act**" means Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2020/1828.

"**Exportable Data and Digital Assets**" (**EDDA**) means Customer Data. EDDA does not include the Provider's trade secrets or intellectual property, or data that could compromise the security or integrity of the Online Application.

"**GDPR**" means 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.

"**Limited Business Operations**" means limited and proportionate operations of the Provider directly related to providing, securing, supporting, billing, managing the contractual relationship, preventing abuse, detecting incidents, complying with legal obligations, internal reporting, financial and accounting settlement, and other similar operational and business purposes necessary for the provision of the Online Application or Professional Services, which do not constitute the processing of Customer Personal Data on the Customer's behalf. Limited Business Operations do not include access to the content of Customer Data or Professional Services Data or analysis of their content for the Provider's own business, marketing, or product development purposes.

"**Local EU/EEA Data Protection Laws**" means subordinate legislation and regulations related to the implementation of the GDPR.

"**Online Application under the European Data Act**" means the Online Application provided to an EU/EEA Customer, excluding the Online Application for which the EU/EEA Customer has elected to store Customer Data outside the EU/EEA.

"**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 person. Pseudonymized or otherwise de-identified data is Personal Data if the natural person remains identifiable under the Data Protection Requirements.

"**Preview Data**" means Customer Data and personal data provided to the Provider by the Customer or on the Customer's behalf through the use of Preview Features, or generated as a result of such use.

"**Preview Features**" means features or versions of the Online Application provided as preview, beta, or experimental, which are not the generally available version of the Online Application.

"**Professional Services**" means Support and any implementation, consulting, advisory, configuration, or other professional activities provided by the Provider to the Customer under the Agreement or another written agreement between the Parties. Professional Services do not include the Online Application.

"**Professional Services Data**" means all data, including text, audio, or image files, provided by the Customer to the Provider or on the Customer's behalf, or otherwise obtained or processed by the Provider for the Customer in the course of providing Professional Services. Professional Services Data does not include Customer Data or Service Data.

"**Regulatory Authority**" means any public authority or supervisory authority competent for the protection of personal data or other legal obligations of the Customer in the relevant jurisdiction, in particular the national supervisory authority for the protection of personal data within the meaning of the GDPR or UK GDPR.

"**Service Data**" has the meaning set out in the "Definitions" article of the Terms. For the purposes of this DPA, Service Data does not constitute Customer Data or Customer Personal Data.

"**Subprocessor**" means any third party engaged by the Provider in the processing of Customer Personal Data in connection with the provision of the Online Application or Professional Services, as described in Article 28 of the GDPR.

"**Switching**" means a one-time transfer of the EU Customer's EDDA from the Online Application under the European Data Act to a cloud services provider other than the Provider, designated by the EU Customer and whose information the EU Customer provides to the Provider, or to the EU Customer's local ICT environment, if the EU Customer terminates the use of the Online Application under the European Data Act.

"**Transfer Mechanism**" means an adequacy decision, standard contractual clauses approved by the European Commission Decision 2021/914/EC of 4 June 2021, the International Data Transfer Addendum issued by the UK Information Commissioner's Office, or another legally permissible mechanism for the international transfer of personal data under the Data Protection Requirements.

"**UK GDPR**" means the GDPR as it forms part of the law of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018, as amended.

2.3 Terms used in this DPA with a lowercase initial letter that are not otherwise defined, such as "processing", "controller", "processor", "data subject", or "personal data breach", have the same meaning as set out in Article 4 of the GDPR.

2.4 Where it is necessary under this DPA to distinguish between Customer Data, Customer Personal Data, and Service Data, their substantive content and purpose of

processing will prevail over their designation in individual provisions of the Agreement. In case of doubt, Customer Personal Data will be considered a subset of Customer Data, and Service Data will be considered a separate category of data processed by the Provider outside the regime of instruction-based processing of Customer Personal Data, unless expressly agreed otherwise.

2.5 Where this DPA uses the term "personal data" in connection with the Provider's obligations as a processor or Subprocessor, this means, for the purposes of this DPA, Customer Personal Data, unless a specific provision expressly provides otherwise.

3 General Terms

3.1 The Provider will comply with all laws and regulations applicable to the provision of the Online Application and Professional Services, including laws relating to security breach notification and Data Protection Requirements. However, the Provider is not responsible for compliance with laws or regulations applicable to the Customer or the Customer's industry that do not generally apply to information technology service providers. The Provider does not determine whether Customer Personal Data includes information subject to specific laws or regulations. All Security Incidents are subject to the terms of the "Provider Assistance" article of this DPA.

3.2 The Customer must comply with all laws and regulations applicable to its use of the Online Application and use of Professional Services, including laws relating to biometric data, confidentiality of communications, and Data Protection Requirements. The Customer is responsible for determining whether the Online Application and Professional Services are suitable for storing and processing information subject to a specific law or regulation, and for using the Online Application and Professional Services in a manner consistent with its legal and regulatory obligations. The Customer is responsible for responding to third-party requests relating to its use of the Online Application or Professional Services, such as requests to remove content in accordance with the Digital Millennium Copyright Act or other applicable laws.

3.3 The Provider does not control or restrict the geographic areas from which the Customer, its users, or persons acting on its behalf access Customer Data or transfer it outside the Online Application environment. The Customer is responsible for such access or transfer.

3.4 For the Online Application provided as a Free Plan, the Provider's obligations under this DPA that go beyond mandatory legal provisions (in particular the obligation to provide assistance with audits, DPIAs, detailed reports, and similar extended obligations) will apply only to the extent set out in the Free Plan Terms.

4 Roles of the Parties

4.1 In relation to Customer Personal Data, the Customer acts as the controller and the Provider acts as the processor, unless expressly stated otherwise in the Agreement or applicable law.

4.2 The Customer agrees that the Agreement (including this DPA), together with the Online Application documentation, the Support Terms, the Customer's use and configuration of the Online Application, the Customer's use of Professional Services, and the Customer's other written instructions, constitutes the Customer's complete documented instructions to the Provider regarding the processing of Customer Personal Data. Any additional or alternative instructions must be agreed in writing.

4.3 In relation to Customer Personal Data that the Customer itself processes as a processor for a third party, the Provider acts as a subprocessor, unless expressly stated otherwise in the Agreement or applicable law. The Customer confirms that its instructions to the Provider, including the engagement of the Provider as a subprocessor, have been authorized by the relevant controller.

4.4 In relation to Service Data and personal data processed as part of Limited Business Operations, the Provider acts as an independent controller to the extent it determines the purposes and means of such processing for legitimate operational, security, support, accounting, contractual, and legal purposes directly related to the provision of the Online Application or Professional Services.

4.5 For the avoidance of doubt, the Parties agree that the processing of Service Data and personal data as part of Limited Business Operations does not constitute the processing of Customer Personal Data on the Customer's behalf, except to the extent expressly stated otherwise in the Agreement or applicable law.

4.6 In the event of a conflict between the qualification of data as Customer Personal Data and their qualification as Service Data, the substantive purpose of processing and the role of the Provider in the relevant processing under this DPA will prevail.

5 Subject Matter, Duration, Nature, and Purpose of Processing

5.1 The subject matter of the processing is the processing of Customer Personal Data by the Provider for the Customer to the extent necessary for the provision of the Online Application or Professional Services.

5.2 The duration of the processing corresponds to the term of the Agreement, unless a legal provision, this DPA, or a technically justified retention regime for backups and archives requires or permits otherwise.

5.3 The nature and purpose of the processing include, in particular, storing, organizing, structuring, making accessible, retrieving, using, transferring, backing up, restoring, supporting, diagnosing, monitoring, securing, managing, exporting, and deleting

Customer Personal Data to the extent necessary for the provision of the Online Application or Professional Services.

5.4 For the purposes of this DPA, providing the Online Application includes, in particular, making available the functions of the Online Application licensed, agreed, or configured for the Customer and used by the Customer or its users, and ensuring the operation, support, diagnostics, security, troubleshooting, updates, maintenance, and improvement of the reliability, functionality, quality, and security of the Online Application, in each case to the extent necessary for its provision.

5.5 For the purposes of this DPA, providing Professional Services includes, in particular, providing Support and other agreed professional activities, troubleshooting, investigating, mitigating, and remedying problems, incidents, and findings identified in the course of providing Professional Services or in connection with the Customer's use of the Online Application, and improving the provision, effectiveness, quality, and security of Professional Services and the Online Application based on such findings, in each case to the extent necessary for the provision of Professional Services.

5.6 Processing under this article is subject to the technical and organizational measures under this DPA and the Data Protection Requirements.

6 Separation of Customer Data, Customer Personal Data, and Service Data

6.1 Customer Data remains under the Customer's control, and the Provider processes it only to the extent necessary for the provision of the Online Application, based on the Customer's instructions expressed through the Agreement, the Customer's use of the Online Application, or other documented instructions of the Customer.

6.2 The Provider ensures the technical and organizational separation of Customer Data between individual Customers using architecture and technical means corresponding to the Provider's current operational model.

6.3 Customer Personal Data constitutes the portion of Customer Data or Professional Services Data that contains Personal Data and is processed by the Provider on the Customer's behalf as a processor or subprocessor under this DPA.

6.4 Service Data does not constitute Customer Data and is not subject to the instruction-based processing regime under this DPA to the extent it is processed by the Provider for Limited Business Operations, security, support, billing, contractual administration, abuse detection, compliance with legal obligations, and other direct operational purposes related to the provision of the Online Application.

6.5 If Service Data contains personal data, such data will be processed only to the extent necessary for the purposes set out in the preceding paragraph and in accordance with the Data Protection Requirements.

6.6 The Customer retains all rights in Customer Data and Professional Services Data. The Provider does not acquire any rights in Customer Data or Professional Services Data, except for the rights necessary to process them in accordance with the Agreement

and this DPA. This does not affect the Provider's rights in the Online Application, documentation, know-how, software, tools, procedures, or other materials of the Provider.

7 Customer Instructions

7.1 The Provider processes Customer Personal Data only on the basis of the Customer's documented instructions contained in the Agreement, this DPA, the Business Proposal, the Online Application documentation, the Support Terms, the Customer's configuration and use of the Online Application, the Customer's use of Professional Services, and the Customer's other written instructions, provided they are not in conflict with legal provisions.

7.2 If the Provider considers that a specific instruction of the Customer infringes the Data Protection Requirements, the Provider will notify the Customer without undue delay.

7.3 The Customer is responsible for ensuring that it has an appropriate legal basis for the processing of Customer Personal Data through the Online Application or Professional Services, and that it fulfills its information and other obligations as a controller.

8 Restrictions on the Use of Customer Personal Data

8.1 Neither the Provider nor any Subprocessor will use or otherwise process Customer Personal Data for user profiling, advertising or similar advertising purposes, market research for the purpose of creating new functionalities, offerings, or products, training, fine-tuning, or improving generally applicable artificial intelligence models, or any other own purposes that are not consistent with the Customer's documented instructions, unless such use is expressly permitted by the Customer in a separate written agreement.

8.2 The Customer is responsible for assessing the appropriateness of inputting personal data into AI functionalities and for establishing reasonable internal rules for their use in accordance with applicable Data Protection Requirements.

9 Confidentiality and Authorized Persons

9.1 The Provider will ensure that persons authorized to process Personal Data are bound by confidentiality or are subject to an appropriate statutory duty of confidentiality.

9.2 The Provider will ensure that authorized persons have access to Personal Data only to the extent necessary for the performance of their work or contractual tasks.

10 Technical and Organizational Measures

10.1 The Provider's technical and organizational measures are set out in the Annex – Security Measures.

11 Provider Assistance

11.1 Taking into account the nature of the processing and the information available to it, the Provider will reasonably assist the Customer, on the Customer's written request, in fulfilling the Customer's obligations under the Data Protection Requirements, in particular with:

(i) responding to data subject requests;
(ii) ensuring the security of processing;
(iii) data protection impact assessments;
(iv) prior consultations with the supervisory authority; and
(v) notifying personal data breaches.

11.2 If the Provider receives a request from a data subject concerning Customer Personal Data processed by the Provider as a processor or subprocessor, the Provider will direct the data subject to the Customer, unless a legal provision requires otherwise. The Customer is responsible for responding to such request.

11.3 If the Provider becomes aware of a breach of security leading to the accidental or unauthorized loss, destruction, alteration, unauthorized disclosure of, or access to Customer Data, Professional Services Data, or Personal Data processed by the Provider (each a "**Security Incident**"), the Provider will, without undue delay and in any event within seventy-two (72) hours after becoming aware of the Security Incident:

(i) notify the Customer of the Security Incident;
(ii) investigate the Security Incident and provide the Customer with reasonable information about the Security Incident; and
(iii) take reasonable measures to mitigate the effects and minimize any damage resulting from the Security Incident.

11.4 Notifications of Security Incidents will be delivered to the Customer in a manner chosen by the Provider, including by email. The Customer is responsible for maintaining current and accurate contact details for notification in the Business Proposal or customer account. The Customer is responsible for complying with its own incident notification obligations under the laws applicable to the Customer, and for fulfilling third-party obligations related to Security Incidents.

11.5 The Provider will use reasonable efforts to assist the Customer in fulfilling its obligations under Article 33 of the GDPR or other applicable laws relating to notification of the Security Incident to the supervisory authority and to data subjects.

11.6 The Customer will notify the Provider without undue delay of any suspected misuse of its Access Accounts or authentication credentials, as well as of any other security events related to the Online Application of which it becomes aware.

11.7 The Provider is not obliged to fulfill the Customer's own statutory obligations as controller, unless expressly required otherwise by this DPA or mandatory legal provisions.

11.8 A notification or response by the Provider to a Security Incident under this article does not mean that the Provider accepts liability or acknowledges fault in connection with the Security Incident.

12 Records of Processing Activities

12.1 To the extent that the GDPR requires the maintenance of records of processing activities related to the Customer, the Customer will provide the relevant information to the Provider upon request and will ensure its accuracy and currency. The Provider may disclose this information to the competent supervisory authority in the situations provided for by the GDPR.

13 Subprocessors

13.1 The Customer grants the Provider general written authorization to engage Subprocessors.

13.2 The Provider will ensure that Subprocessors are subject to obligations substantially equivalent to those imposed on the Provider by this DPA, in particular regarding confidentiality, security, and the protection of Personal Data.

13.3 The Provider will notify the Customer of intended material changes to the list of Subprocessors by publication on the Provider's website or through a notification mechanism, within a reasonable period in advance.

13.4 If the Customer does not approve a new Subprocessor, the Customer may terminate the affected part of the Online Application or Professional Services for which the new Subprocessor is to be used by written notice before the expiry of the applicable notice period.

13.5 The Provider remains responsible to the Customer for the performance of its Subprocessors' obligations to the extent required by the Data Protection Requirements.

13.6 The Provider may fulfill the information obligations under this article also by reference to the current list of Subprocessors, an overview of the main categories of Subprocessors, the Trust Center, or a similar interface, provided that such method gives the Customer reasonable access to the relevant information.

14 Public Authority Requests

14.1 If the Provider is legally required to disclose Personal Data to a public authority, Regulatory Authority, or other authorized entity, the Provider will inform the Customer without undue delay before such disclosure, unless prohibited by law.

14.2 The Provider will limit the scope of such disclosure to the minimum legally necessary and will reasonably assist the Customer in assessing the impact of such request.

14.3 If the Personal Data is processed through Microsoft or another Subprocessor, the Provider may fulfill the information obligation under this article also by reference to the relevant contractual or operational mechanisms of such Subprocessor, where the nature of the matter permits.

14.4 The Provider will not disclose Customer Personal Data to third parties, except where:

(i) the Customer instructs it to do so,

(ii) this results from this DPA, or

(iii) it is required by law. The Provider will attempt to redirect the third party with the request for disclosure of Customer Personal Data directly to the Customer.

14.5 The Provider will not provide any third party with:

(i) direct, indirect, or unrestricted access to Customer Personal Data;

(ii) encryption keys used to protect it; or

(iii) access to Customer Personal Data if it knows that it is to be used for purposes other than those set out in the third party's request. Disclosure of data based on a legal provision is permissible only if such legal provision respects the essence of fundamental rights and freedoms and does not exceed what is necessary in a democratic society.

15 Transfers to Third Countries

15.1 The Provider may transfer Personal Data to third countries or international organizations only if the conditions set out in the Data Protection Requirements are met.

15.2 Where required by the Data Protection Requirements, the Provider will ensure an appropriate legal Transfer Mechanism for such transfer; for transfers from the United Kingdom, the IDTA (International Data Transfer Addendum issued by the UK ICO under section 119A(1) of the Data Protection Act 2018) will additionally apply.

15.3 Transfers of Customer Personal Data from the United Kingdom to a Member State of the European Union or the European Economic Area do not require standard contractual clauses or a separate transfer impact assessment, provided that the United Kingdom maintains an adequacy regime or other equivalent legal basis for the country concerned.

16 Audits and Information

16.1 The Provider conducts audits of the security of the computers, computing environment, and physical data centers that Provider uses in processing Customer Personal Data, as follows:

(i) where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually;

(ii) each audit will be performed in accordance with the standards and rules of the regulatory or accreditation body for each applicable control standard or framework;

(iii) each audit will be performed by qualified, independent third-party security auditors selected by Provider and at Provider's expense.

16.2 Each audit will result in the generation of an audit report (the "**Audit Report**"). The Audit Report is Provider's Confidential Information and will clearly disclose any material findings by the auditor. Provider will promptly remediate issues raised in the Audit Report to the satisfaction of the auditor. Upon Customer's written request and subject to a non-disclosure agreement, Provider will provide Customer with a summary copy of the Audit Report. The Audit Report is subject to non-disclosure and distribution limitations of Provider and the auditor.

16.3 To the extent Customer's audit requirements under the Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation, or compliance information that Provider generally makes available to its customers, Provider will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, the Parties will mutually agree upon the scope, timing, duration, control, evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Provider to unreasonably delay performance of the audit.

16.4 To the extent needed to perform the audit, Provider will make available the processing systems, facilities, and supporting documentation relevant to the processing of Customer Personal Data by Provider, its Affiliates, and its Subprocessors. Such audit will be conducted by an independent, accredited third-party audit firm, during Provider's regular business hours, with reasonable advance notice to Provider, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor will have access to data of Provider's other customers or to systems, facilities, or documentation of Provider not involved in providing the Online Application or Professional Services to Customer. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Provider expends for any such audit, in addition to the rates for activities performed by Provider. If the audit report generated as a result of Customer's audit identifies any material non-compliance, Customer will share such audit report with Provider, and Provider will promptly cure any material non-compliance.

16.5 Provider may require that the auditor is not a direct competitor of Provider. Provider is not obliged to permit physical access to third-party premises, disclose source code, internal security know-how, confidential information of other customers, or any other information beyond the scope of reasonableness, proportionality, and protection of confidential information.

16.6 Nothing in this section varies or modifies Provider's obligations under the GDPR or other Data Protection Requirements and does not affect the rights of supervisory authorities or data subjects under those requirements.

17 Preview Versions

17.1 For Preview Features that enable the processing of Personal Data, all terms of this DPA apply, except that Preview Data may be transferred, stored, and processed outside the EU/EEA in countries where the Provider or its Subprocessors operate, unless the Provider expressly specifies otherwise.

17.2 The Provider will ensure that Preview Data is not retained after termination of the relevant Preview feature.

17.3 Preview Features may be subject to additional terms provided separately.

17.4 The Provider's obligations under the European Data Act apply to Preview Features only to the extent expressly required by mandatory law or to the extent their application is expressly agreed in the Business Proposal.

18 European Data Act

18.1 Switching is permitted at any time without additional costs beyond the fees and other amounts otherwise payable under the Agreement with the EU Customer. The EU Customer may access, export and delete EDDA at any time, including access to and export of EDDA for the period set out in the article Duration and Termination of the Agreement of the Terms. As part of Switching, EDDA will be made available to the EU Customer for download in the form of a standard SQL database backup. The EU Customer decides when and within what time frame to initiate the export of EDDA. Depending on the Customer's specific configuration, the amount of data, the switching destination and other circumstances beyond the Provider's control, the actual extraction and export of EDDA by the EU Customer may take more than 30 days. The EU Customer should complete Switching before terminating the Online Application under the European Data Act, which the EU Customer may do by giving the Provider 60 days' notice and paying any amount that it may still owe under the Agreement with the EU Customer. The Provider will provide reasonable assistance with Switching and will exercise due care, as set out in the Technical and Organizational Measures article of this DPA and under the Agreement, when providing the Online Application under the European Data Act during Switching and during parallel use. For the avoidance of doubt, repayment of the discount from the price of the Online Application expressly agreed in the Agreement constitutes solely an adjustment of the price for the period during which the Online Application was actually provided to the standard price without the agreed discount and does not constitute an additional charge under this paragraph or a charge for Switching, export of EDDA or parallel use. These conditions do not apply to Preview Features.

18.1 Supporting materials on data export and methods and information concerning the Provider's ICT infrastructure used for providing the Online Application under the European Data Act and the manner in which the Provider responds to requests from public authorities for access to data are available in the Online Application documentation at https://doc.alvao.com.

19 Return, Deletion, and Backups

19.1 After termination of the Agreement, the Parties will act in accordance with the Duration and Termination of the Agreement article of the Terms, unless this DPA or a legal provision provides otherwise.

19.2 Upon cessation of the provision of the Online Application or Professional Services, the Provider will, at the Customer's instruction, return or delete Personal Data, unless a legal provision or a technically justified retention regime for backups and archives requires or permits otherwise.

19.3 If Personal Data is contained in backups or archives that cannot be technically removed immediately, such data may be retained until the expiry of the regular retention cycle, but during this period it will not be actively used, except in cases of recovery, security, compliance with a legal obligation, or exercise or defense of legal claims.

19.4 The Provider will remove Professional Services Data from its active systems after fulfilling the business purposes for which it was collected or provided, or earlier upon the Customer's written request, unless a legal provision or this DPA entitles the Provider to further retention.

20 Service Data

20.1 To the extent that Service Data contains Personal Data, the Provider may process such Service Data to the extent necessary for Limited Business Operations, in particular for providing, securing, monitoring, supporting, billing, contractual administration, abuse prevention, incident detection, compliance with legal obligations, and protection of its rights in connection with the Online Application.

20.2 Service Data may be stored and processed in the territory of the EU/EEA regardless of the selected data location for Customer Data.

20.3 The Provider will limit the scope of Service Data to the minimum reasonably necessary for the stated purposes and will not use Service Data containing Personal Data for general marketing purposes, sales profiling, training generally applicable artificial intelligence models, or other own purposes unrelated to the provision of the Online Application.

20.4 Service Data does not constitute Customer Data or Customer Personal Data and is not subject to instruction-based processing under this DPA. If Service Data contains Personal Data, the Provider processes such Personal Data as an independent controller to the extent necessary for Limited Business Operations and exclusively for legitimate operational, security, support, contractual, and legal purposes.

21 Business Associate (HIPAA)

21.1 If the Customer intends to include "protected health information" within the meaning of HIPAA in Customer Data or Professional Services Data, it must ensure in advance

that the Parties have expressly entered into a separate HIPAA Business Associate Agreement. If no such agreement has been entered into, neither the Online Application nor Professional Services are intended for the processing of "protected health information" within the meaning of HIPAA, and the Provider does not assume the status of a Business Associate under HIPAA in relation to such information.

22 Educational Institutions (FERPA)

22.1 If the Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g ("FERPA"), apply, the Provider acknowledges that for the purposes of this DPA, the Provider is a "school official" with "legitimate educational interests" in the Customer Data and Professional Services Data, as those terms have been defined under FERPA and its implementing regulations, and the Provider agrees to abide by the limitations and requirements imposed by 34 CFR § 99.33(a) on school officials.

22.2 The Customer acknowledges that the Provider may have limited or no contact information for the Customer's students and students' parents. The Customer is therefore responsible for obtaining any parental consent for any end user's use of the Online Application required by applicable law and for conveying notification on behalf of the Provider to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data or Professional Services Data in the Provider's possession as may be required under applicable law.

23 California Consumer Privacy Act (CCPA)

23.1 If the processing of Customer Personal Data is subject to the CCPA, the Provider acts as a "Service Provider" within the meaning of the CCPA, and such data: (i) will not be retained, used, or transferred beyond this DPA; (ii) will not be sold or shared in any event within the meaning of the CCPA; and (iii) will not be combined with personal data obtained from other sources, unless expressly permitted by the CCPA.

24 Biometric Data

24.1 If the Customer uses the Online Application or Professional Services to process biometric data within the meaning of Article 4 of the GDPR or applicable Data Protection Requirements, the Customer is responsible for informing data subjects, obtaining their consent, and deleting biometric data. The Provider processes biometric data exclusively according to the Customer's instructions and in accordance with this DPA.

25 Contact Persons

25.1 The Parties may designate contact persons for matters of Personal Data protection, security, and incidents. If none are designated, the general contact details under the Communication Between the Parties article of the Terms will apply.

26 Change of the DPA

26.1 The Provider reserves the right to unilaterally amend this DPA, including its annexes. The Customer will be notified of such amendment by publication of the updated version of the DPA on the Provider's website or by another demonstrable means.

26.2 This DPA will not change during the term of the Subscription or the term of the relevant Professional Services commitment. Upon renewal or entry into a new Subscription, or upon renewal or entry into a new Professional Services commitment, the DPA then in effect will apply, unless mandatory law provides otherwise.

26.3 If a change of the DPA would materially worsen the Customer's legal position in relation to the already agreed scope of processing, the Customer may notify the Provider that it does not wish to renew the Subscription or the relevant Professional Services commitment, no later than the day preceding the day of its renewal.

26.4 Notwithstanding the limitations on changes to the DPA under this article, the Provider may provide new or updated DPA terms for new features, offerings, add-ons, or related software that were not previously included in the Online Application or Professional Services, where such terms apply to their use. If such terms include a materially adverse change to the DPA, the Provider will allow the Customer not to use those new features, offerings, add-ons, or related software without losing the ability to use the existing generally available features of the Online Application or the agreed Professional Services. If the Customer does not use such new features, offerings, add-ons, or related software, the corresponding new or updated terms will not apply to the Customer.

26.5 Previous versions of the DPA will be provided to the Customer upon request or will be available on the Provider's website.

27 Final Provisions

27.1 This DPA survives for the duration of the Provider's processing of Customer Personal Data on behalf of the Customer.

27.2 Unless this DPA, the Agreement, or mandatory law provides otherwise, each Party bears its own costs incurred in the performance of obligations under this DPA.

27.3 This version of the DPA is effective as of July 1, 2026.

Annex – Security Measures

1 Technical and Organizational Measures

1.1 The Provider will implement and maintain technical and organizational measures appropriate to the nature, scope, context, and purposes of processing Customer Personal Data and to the risks to the rights and freedoms of natural persons.

1.2 These measures include, in particular:

(i) access control to Customer Personal Data based on the principle of least privilege and role-based access control;

(ii) contractual or statutory confidentiality obligations of persons authorized to process Customer Personal Data;

(iii) measures to ensure the confidentiality, integrity, availability, and resilience of processing systems and services;

(iv) encryption of data in transit and, depending on the nature of the Online Application, also encryption of data at rest;

(v) logging, monitoring, and recording of security-relevant events;

(vi) procedures for detecting, responding to, and reporting Security Incidents and Personal Data Breaches;

(vii) processes for vulnerability management, updates, and security maintenance of the infrastructure and software used;

(viii) measures for backup, recovery, and business continuity appropriate to the nature of the Online Application provided;

(ix) processes for assessing and managing Subprocessors;

(x) regular review, testing, and evaluation of the effectiveness of the technical and organizational measures implemented.

1.3 The Provider ensures that the processing of Customer Personal Data is subject to reasonable technical and organizational measures implemented and maintained by the Provider and its Affiliates involved in the provision and operation of the Online Application. These measures form part of the information security management system and related control environment, which have successfully passed or hold certifications and assessments including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and SOC 2 Type 2. The Provider may continuously renew, replace, or expand these certifications, assessments, and related control frameworks with newer or equivalent versions, provided that this does not materially reduce the level of protection of Customer Personal Data.

1.4 The Provider may fulfill the information obligations regarding technical and organizational measures also through the Trust Center, security documentation, audit reports, certifications, or other reasonable evidentiary means, provided that such method gives the Customer reasonable access to the relevant information and is consistent with the Agreement.

Annex – Data Subjects and Categories of Personal Data

1 Categories of Data Subjects

1.1 In connection with the provision of the Online Application or Professional Services, the Provider may process Personal Data of the following categories of data subjects to the extent determined by the Customer:

(i) employees, workers, and collaborators of the Customer;

(ii) customers, business partners, suppliers, and other contact persons of the Customer;

(iii) users, administrators, and other persons to whom the Customer enables the use of the Online Application;

(iv) other natural persons whose Personal Data the Customer inputs into the Online Application or otherwise makes available to the Provider.

2 Categories of Personal Data

2.1 In connection with the provision of the Online Application or Professional Services, the Provider may process, in particular, the following categories of Personal Data:

(i) identification and contact details;

(ii) job or functional position;

(iii) access and authentication credentials;

(iv) data contained in support requests, incidents, tickets, attachments, diagnostic outputs, and communication records;

(v) technical and operational data related to the provision of the Online Application;

(vi) other Personal Data that the Customer inputs into the Online Application or otherwise makes available to the Provider.

3 Special Categories of Personal Data

3.1 The Customer determines and controls the content of the Personal Data it inputs into the Online Application or otherwise makes available to the Provider. Such Personal Data may include special categories of Personal Data or other specially protected Personal Data only to the extent determined by the Customer and in accordance with the Data Protection Requirements.