Version 1.0
Last Updated: February 26, 2025

Alaigned Data Processing Addendum

This Data Processing Addendum represents an addendum to Customer's (also referred as "**You**") existing commercial agreement with Alaigned (also referred as "**Provider**") governing Customer's use of Provider products or Services ("**Agreement**") (each, a "**Party**" and together, the "**Parties**") ("**Addendum**"/"**DPA**") and is hereby incorporated into the Agreement. In the event of any conflict between this Addendum and any data processing terms contained in the Agreement between the Parties, the terms of this Addendum regarding the transfer of Personal Data shall control and supersede the terms set forth in the Agreement.

1. Definitions.

All capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement or the Applicable Data Protection Law, as applicable.

1.1. "**Audit**" and "**Audit Parameters**" are defined in Section 9.3. below.

1.2. "**Audit Report**" is defined in Section 9.2. below.

1.3. "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data.

1.4. "**Customer Instructions**" is defined in Section 3.1. below.

1.5. "**Customer Personal Data**" means Personal Data in Customer Data (as defined in the Agreement).

1.6. "**Data Protection Laws**" means all laws and regulations applicable to the Processing of Customer Personal Data under the Agreement, including, as applicable: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any binding regulations promulgated thereunder ("**CCPA**"), (ii) the General Data Protection Regulation (Regulation (EU) 2016/679) ("**EU GDPR**" or "**GDPR**"), (iii) the Swiss Federal Act on Data Protection ("**FADP**"), (iv) the EU GDPR as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (the "**UK GDPR**") and (v) the UK Data Protection Act 2018; in each case, as updated, amended or replaced from time to time.

1.7. "**Data Subject**" means the identified or identifiable natural person to whom Customer Personal Data relates.

1.8. "**EEA**" means European Economic Area.

1.9. "**Personal Data**" means information about an identified or identifiable natural person or which otherwise constitutes "personal data", "personal information", "personally identifiable information" or similar terms as defined in Data Protection Laws.

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

1.11. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

1.12. "**Restricted Transfer**" means: (i) where EU GDPR applies, a transfer of Customer Personal Data from the EEA to a country outside the EEA that is not subject to an adequacy determination, (ii) where UK GDPR applies, a transfer of Customer Personal Data from the United Kingdom to any other country that is not subject to an adequacy determination or (iii) where FADP applies, a transfer of Customer Personal Data from Switzerland to any other country that is not subject to an adequacy determination.

1.13. "**Services**" means: Subscription Services and Professional Services (as defined in the Agreement).

1.14. "**Schedules**" means one or more schedules incorporated by the Parties to this Addendum. The default Schedules for this Addendum are:

Schedule 1	Subject Matter and Details of Processing
Schedule 2	Technical and Organizational Measures
Schedule 3	Cross-Border Transfer Mechanisms
Schedule 4	Region-Specific Terms

1.15. "**Security Incident**" means any breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data being Processed by Provider.

1.16. "**Specified Notice Period**" is 48 hours.

1.17. "**Subprocessor**" means any third party authorized by Provider to Process any Customer Personal Data.

1.18. "**Subprocessor List**" means the list of Provider's Subprocessors as listed at https://alaigned.com/subprocessors.

2. Scope and Duration.

2.1. **Roles of the Parties**. This DPA applies to Provider as a Processor of Customer Personal Data and to Customer as a Controller or Processor of Customer Personal Data.

2.2. **Scope of DPA**. This DPA applies to Provider's Processing of Customer Personal Data under the Agreement to the extent such Processing is subject to Data Protection Laws. This DPA is governed by the governing law of the Agreement unless otherwise required by Data Protection Laws.

2.3. **Duration of DPA**. This DPA terminates upon expiration or termination of the Agreement (or, if later, the date on which Provider has ceased all Processing of Customer Personal Data).

2.4. **Order of Precedence**. In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) any Standard Contractual Clauses or other measures to which the Parties have agreed in Schedule 3 (Cross-Border Transfer Mechanisms) or Schedule 4 (Region-Specific Terms) (if applicable), (2) this DPA and (3) the Agreement. To the fullest extent permitted by Data Protection Laws, any claims brought in connection with this DPA (including its Schedules) will be subject to the terms and conditions, including, but not limited to, the exclusions and limitations, set forth in the Agreement.

3. Processing of Personal Data.

3.1. **Customer Instructions**.

(a) Provider will Process Customer Personal Data as a Processor only: (i) in accordance with Customer Instructions or (ii) to comply with Provider's obligations under applicable laws, subject to any notice requirements under Data Protection Laws.

(b) "**Customer Instructions**" means: (i) Processing to provide Services and perform Provider's obligations in the Agreement (including this DPA) and (ii) other reasonable documented instructions of Customer consistent with the terms of the Agreement.

(c) Details regarding the Processing of Customer Personal Data by Provider are set forth in Schedule 1 (Subject Matter and Details of Processing).

(d) Provider will notify Customer if it receives an instruction that Provider reasonably determines infringes Data Protection Laws (at the same time, Provider has no obligation to actively monitor Customer's compliance with Data Protection Laws).

3.2. **Confidentiality**.

(a) Provider will protect Customer Personal Data in accordance with its confidentiality obligations as set forth in the Agreement.

(b) Provider will ensure personnel who Process Customer Personal Data (including Provider's Affiliates, staff, agents and subcontractors) either enter into written confidentiality agreements or are subject to statutory obligations of confidentiality.

3.3. **Compliance with Laws**.

(a) Provider and Customer will each comply with Data Protection Laws in their respective Processing of Customer Personal Data.

(b) Customer will comply with Data Protection Laws in its issuing of Customer Instructions to Provider. Customer will ensure that it has established all necessary lawful bases under Data Protection Laws to enable Provider to lawfully Process Customer Personal Data for the purposes contemplated by the Agreement (including this DPA), including, as applicable, by obtaining all necessary consents from, and giving all necessary notices to, Data Subjects.

3.4. **Changes to Laws**. The Parties will work together in good faith to negotiate an amendment to this DPA as either Party reasonably considers necessary to address the requirements of Data Protection Laws from time to time.

4. Subprocessors.

4.1. **Use of Subprocessors**.

(a) Customer generally authorizes Provider to engage Subprocessors to Process Customer Personal Data. Customer further agrees that Provider may engage its Affiliates as Subprocessors.

(b) Provider will: (i) enter into a written agreement with each Subprocessor imposing data Processing and protection obligations substantially the same as those set out in this DPA and (ii) remain liable for compliance with the obligations of this DPA and for any acts or omissions of a Subprocessor that cause Provider to breach any of its obligations under this DPA.

4.2. **Subprocessor List**. Provider will maintain an up-to-date list of its Subprocessors, including their functions and locations, as specified in the Subprocessor List.

4.3. **Notice of New Subprocessors**. Customer authorizes Provider to add and/or modify its Subprocessor List, on the condition that Provider furnishes at least thirty (30) days' prior written notice of the addition and/or modification of any Subprocessor (including the categories of Personal Data processed, details of the Processing it performs or will perform, and the location of such Processing) by means of a notice on the aforementioned Subprocessor List site. Provider encourages Customer to periodically review the Provider's Subprocessor List for the latest information on Provider's Subprocessor practices, and especially before Customer provides Provider with any Personal Data. Customer may sign up to receive email notification of any such changes to the Subprocessor List on the https://alaigned.com/subprocessors site.

4.4. **Objection to New Subprocessors**.

(a) If, within 30 days after written notice of a new Subprocessor, Customer notifies Provider in writing that Customer objects to Provider's appointment of such new Subprocessor based on reasonable data protection concerns, the Parties will discuss such concerns in good faith to either resolve the concerns or to identify alternate arrangements to allow for continued Processing of Customer Personal Data by Provider.

(b) Customer's continued use of Provider's Services thirty (30) days after any changes or revisions to the Subprocessor List have been published shall indicate its agreement with the terms of such revised list.

5. Security.

5.1. **Security Measures**. Provider will implement and maintain reasonable and appropriate technical and organizational measures, procedures and practices, as appropriate to the nature of the Customer Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Customer Personal Data and protect against Security Incidents, in accordance with Provider's Security Procedures referenced in the Agreement and as further described in Schedule 2 (Technical and Organizational Measures). Provider will regularly monitor its compliance with its Security Measures and Schedule 2 (Technical and Organizational Measures).

5.2. **Incident Notice and Response**.

(a) Provider will implement and follow procedures to detect and respond to Security Incidents.

(b) Provider will: (i) notify Customer without undue delay and, in any event, not later than the Specified Notice Period, after becoming aware of a Security Incident affecting Customer and (ii) make reasonable efforts to identify the cause of the Security Incident, mitigate the effects and remediate the cause to the extent within Provider's reasonable control.

(c) Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by providing, when available, additional information reasonably necessary for Customer to meet its Security Incident notification obligations under Data Protection Laws.

(d) Customer acknowledges that Provider's notification of a Security Incident is not an acknowledgement by Provider of its fault or liability.

(e) For the sake of clarity, Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including but not limited to unsuccessful login attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

5.3. **Customer Responsibilities.**

(a) Customer is responsible for reviewing the information made available by Provider relating to data security and making an independent determination as to whether the Services provided under Agreement meets Customer's requirements and legal obligations under Data Protection Laws.

(b) Customer is solely responsible for complying with Security Incident notification laws applicable to Customer and fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents.

6. Data Protection Impact Assessment. Upon Customer's request and taking into account the nature of the applicable Processing, to the extent such information is available to Provider, Provider will assist Customer in fulfilling Customer's obligations under Data Protection Laws to carry out a data protection impact or similar risk assessment related to Customer's use of the Services, including, if required by Data Protection Laws, by assisting Customer in consultations with relevant government authorities.

7. Data Subject Requests.

7.1. **Assisting Customer**. Upon Customer's request and taking into account the nature of the applicable Processing, Provider will assist Customer by appropriate technical and organizational measures, insofar as possible, in complying with Customer's obligations under Data Protection Laws to respond to requests from individuals to exercise their rights under Data Protection Laws, provided that Customer cannot reasonably fulfill such requests independently (including through use of the Services).

7.2. **Data Subject Requests**. If Provider receives a request from a Data Subject in relation to the Data Subject's Customer Personal Data, Provider will notify Customer and advise the Data Subject to submit the request to Customer (but not otherwise communicate with

the Data Subject regarding the request except as may be required by Data Protection Laws), and Customer will be responsible for responding to any such request.

8. Data Return or Deletion.

8.1. **During Subscription Term**. During the Subscription Term, Customer may, through the features of the Services, access, return to itself or delete Customer Personal Data. In addition, Provider will delete all Customer Personal Data at any time during the Subscription Term upon a Customer written request.

8.2. **Post Termination**.

(a) Following termination or expiration of the Agreement, Provider will, in accordance with its obligations under the Agreement, delete all Customer Personal Data from Provider's systems.

(b) Deletion will be in accordance with industry-standard secure deletion practices. Provider will issue a certificate of deletion upon Customer's written request.

(c) Notwithstanding the foregoing, Provider may retain Customer Personal Data: (i) as required by Data Protection Laws or (ii) in accordance with its standard backup or record retention policies, provided that, in either case, Provider will (x) maintain the confidentiality of, and otherwise comply with the applicable provisions of this DPA with respect to, retained Customer Personal Data and (y) not further Process retained Customer Personal Data except for such purpose(s) and duration specified in such applicable Data Protection Laws.

9. Audits.

9.1. **Provider Records Generally**. Provider will keep records of its Processing in compliance with Data Protection Laws and, upon Customer's request, make available to Customer any records reasonably necessary to demonstrate compliance with Provider's obligations under this DPA and Data Protection Laws.

9.2. **Compliance Program**.

(a) Provider will describe its internal and/or third-party audit and certification programs (if any) and make summary copies of its audit reports (each, an "**Audit Report**") available to Customer upon Customer's written request on an annual basis and subject to confidentiality obligations.

(b) Customer may share a copy of Audit Reports with relevant government authorities as required upon their request.

(c) Customer agrees that any audit rights granted by Data Protection Laws will be satisfied by Audit Reports and the procedures of Section 9.3. (Customer Audit) below.

9.3. **Customer Audit**.

(a) Subject to the terms of this Section 9.3., Customer has the right, at Customer's expense, to conduct an audit of reasonable scope and duration pursuant to a mutually agreed-upon audit plan with Provider that is consistent with the Audit Parameters (an "**Audit**").

(b) Customer may exercise its Audit right: (i) to the extent Provider's provision of an Audit Report does not provide sufficient information for Customer to verify Provider's compliance with this DPA and the Data Protection Laws, (ii) as necessary for Customer to respond to a government authority audit or (iii) in connection with a Security Incident.

(c) Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) Be limited in scope to matters reasonably required for Customer to assess Provider's compliance with this DPA and the Data Protection Laws, (ii) occur at a mutually agreed date and time and only during Provider's regular business hours, (iii) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (iv) cover only facilities controlled by Provider, (v) restrict findings to Customer Personal Data only and (vi) treat any results as Confidential Information to the fullest extent permitted by Data Protection Laws.

(d) Customer will reimburse Provider for reasonably incurred costs related to the Audit; the rates are to be negotiated in good faith ahead of the Audit, except in case the Audit is conducted in connection with a Security Incident or upon a specific written request by a government authority.

10. Cross-Border Transfers/Region-Specific Terms.

10.1. **Cross-Border Data Transfers**.

(a) Provider (and its Affiliates) may Process and transfer Customer Personal Data globally as necessary to provide the Services under the Agreement.

(b) If Provider engages in a Restricted Transfer, it will comply with Schedule 3 (Cross-Border Transfer Mechanisms).

10.2. **Region-Specific Terms**. To the extent that Provider Processes Customer Personal Data protected by Data Protection Laws in one of the regions listed in Schedule 4 (Region-Specific Terms), then the terms specified therein with respect to the applicable jurisdiction(s) will apply in addition to the terms of this DPA.

11. Liability.

11.1. **Liability Cap**. Subject to Section 11.2. (Liability Cap Exclusions), the total combined liability of either Party and its Affiliates towards the other Party and its Affiliates under or

in connection with the Agreement and this Addendum combined will be limited to the agreed Liability Cap for the relevant Party under the Agreement.

11.2. **Liability Cap Exclusions**. Nothing in Section 11.1. (Liability Cap) will affect the remaining terms of the Agreement relating to liability (including any specific exclusions from any limitation of liability).

Schedule 1: Subject Matter and Details of Processing

Provider / 'Data Exporter' Details

Name:	Alaigned s.r.o.
Contact details for data protection:	Radovan Janeček, CEO privacy@alaigned.com
Main address:	Na Strži 2102/61a 140 00 Prague 4 Czechia
Provider activities:	Performance of the Agreement
Role:	Processor

Provider / 'Data Importer' Details

Name:	Customer (as defined in the Agreement)
Contact details for data protection:	(as provided by Customer during registration or in the Agreement)
Main address:	(as provided by Customer in the Agreement)
Customer activities:	Performance of the Agreement
Role:	Controller

Alaigned

Details of Processing

Categories of Data Subjects:	Customers, Prospects, Business Partners and Employees and Contractors of the Customer
Categories of Customer Personal Data:	First and Last Name Title and Employer Business Contact Information Personal Contact Information Email Content
Sensitive Categories of Data and additional associated restrictions/safeguards:	No Sensitive Categories of Data will be transferred
Frequency of transfer:	Ongoing
Nature of the Processing:	Storing, analyzing, combining, enriching, and distributing of Personal Data to perform Services under the Agreement
Purpose of the Processing:	Performance of the Agreement
Duration of Processing / retention period:	For the duration of the Agreement
Transfers to Subprocessors:	As per Subprocessors List

Schedule 2: Technical and Organizational Measures

1. Physical Access Controls: the Processor shall take reasonable measures to prevent physical access, such as security personnel and secured buildings and factory premises, to prevent unauthorized persons from gaining access to Personal Data.

2. System Access Controls: the Processor shall implement appropriate measures to prevent unauthorized use of Personal Data. These controls shall be proportionate to the nature of the Processing and may include, but are not limited to, authentication mechanisms, access management procedures, and monitoring of system activity.

3. Data Access Controls: the Processor shall take reasonable measures to provide that Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted and application access rights are established and enforced to ensure that persons entitled to use a data Processing system only have access to the Personal Data to which they have privilege of access; and, that Personal Data cannot be read, copied, modified or removed without authorization in the course of Processing. In addition to the access control rules set forth in Sections 1–3 above, the Processor implements an access policy under which access to its system environment, to Personal Data and other data is restricted to authorized personnel only.

4. Transmission Controls: the Processor shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

5. Input Controls: the Processor shall take reasonable measures to provide that it is possible to check and establish whether and by whom Personal Data has been entered into data Processing systems, modified or removed. The Processor shall take reasonable measures to ensure that (i) the Personal Data source is under the control of the Controller; and (ii) Personal Data integrated into Processor's systems is managed by secured file transfer from the Controller and Data Subject.

6. Data Backup: the Processor shall ensure that back-ups are taken on a regular basis, are secured, and encrypted when storing Personal Data to protect against accidental destruction or loss when hosted by the Processor.

7. Logical Separation: the Processor shall ensure that data from the Controller is logically segregated on the Processor's systems to ensure that Personal Data that is collected for different purposes may be processed separately.

8. Shared Responsibilities for Information Security: Controller agrees that in accordance with applicable Data Protection Laws and before submitting any Personal Data to the Services, Controller will perform an appropriate risk assessment to determine whether the Security Measures within the Services provide an adequate level of security, taking into account the nature, scope, context and purposes of the Processing, the risks associated with the Personal Data and the applicable Data Protection Laws. Upon Controller's written request, Processor will provide Controller reasonable assistance by providing Controller with information requested by Controller to conduct security risk assessment. Controller is solely responsible for determining the adequacy of the Security Measures within the Services in relation to the Customer Personal Data Processed.

Schedule 3: Cross-Border Transfer Mechanisms

1. Definitions. Capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "**EU Standard Contractual Clauses**" or "**EU SCCs**" means the annex found in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (available as of the Addendum effective date at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj or any subsequent link published by the competent EU authorities). In the event of any conflict between the EU Standard Contractual Clauses and this Addendum, the EU Standard Contractual Clauses shall control and supersede.

1.2. "**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force as of March 21, 2022.

1.3. In addition:

"**Designated EU Governing Law**" means: "**Designated EU Member State**" means:	Law of Czechia Czechia

2. EU Transfers. Where Customer Personal Data is protected by EU GDPR and is subject to a Restricted Transfer, the following applies:

2.1. The EU SCCs are hereby incorporated by reference as follows:

(a) Module 3 (Processor to Processor) applies where Provider is a Processor of Customer Personal Data and Customer is a Processor of Customer Personal Data (on behalf of a third-party Controller);

(b) Module 4 (Processor to Controller) applies where Provider is a Processor of Customer Personal Data and Customer is a Controller of Customer Personal Data;

(c) Provider is the "data exporter" and Customer is the "data importer"; and

(d) by entering into this DPA, each Party is deemed to have signed the EU SCCs (including their Annexes) as of the DPA Effective Date.

2.2. For each Module, where applicable the following applies:

(a) the optional docking clause in Clause 7 does not apply;

(b) in Clause 9, Option 2 will apply, the minimum time period for prior notice of Subprocessor changes shall be as set out in Section 4.3. of this DPA, and Provider shall fulfill its notification obligations by notifying Customer of any Subprocessor changes in accordance with Section 4.3. of this DPA;

(c) in Clause 11, the optional language does not apply;

(d) in Clause 13, all square brackets are removed with the text remaining;

(e) in Clause 17, the EU SCCs will be governed by Designated EU Governing Law; (i.e. for Module 3 Option 1 will apply);

(f) in Clause 18, disputes will be resolved before the courts of the Designated EU Member State; (i.e. for Module 3 section (b) will apply);

(g) Schedule 1 (Subject Matter and Details of Processing) to this DPA contains the information required in Annex 1 of the EU SCCs; and

(h) Schedule 2 (Technical and Organizational Measures) to this DPA contains the information required in Annex 2 of the EU SCCs.

(i) Competent Supervisory Authority in Accordance with Clause 13 is the Czech Perosnal Data Protection Office with its address at Pplk. Sochora 27. 170 00 Prague 7, Czech Republic.

2.3. Where context permits and requires, any reference in this DPA to the EU SCCs shall be read as a reference to the EU SCCs as modified in the manner set forth in this Section 2.

3. Swiss Transfers. Where Customer Personal Data is protected by the FADP and is subject to a Restricted Transfer, the following applies:

3.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

(a) in Clause 13, the competent supervisory authority shall be the Swiss Federal Data Protection and Information Commissioner;

(b) in Clause 17, the EU SCCs will be governed by the laws of Switzerland;

(c) in Clause 18, disputes will be resolved before the courts of Switzerland;

(d) the term Member State must not be interpreted in such a way as to exclude Data Subjects in Switzerland from enforcing their rights in their place of habitual residence in accordance with Clause 18(c); and

(e) all references to the EU GDPR in this DPA are also deemed to refer to the FADP.

4. UK Transfers. Where Customer Personal Data is protected by the UK GDPR and is subject to a Restricted Transfer, the following applies:

4.1. The EU SCCs apply as set forth in Section 2 (EU Transfers) of this Schedule 3 with the following modifications:

(a) each Party shall be deemed to have signed the "UK Addendum to the EU Standard Contractual Clauses" ("**UK Addendum**") issued by the Information Commissioner's Office under section 119 (A) of the Data Protection Act 2018;

(b) the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of Customer Personal Data;

(c) in Table 1 of the UK Addendum, the Parties' key contact information is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(d) in Table 2 of the UK Addendum, information about the version of the EU SCCs, modules and selected clauses which this UK Addendum is appended to are located above in this Schedule 3;

(e) in Table 3 of the UK Addendum:

(i) the list of Parties is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(ii) the description of transfer is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA;

(iii) Annex II is located in Schedule 2 (Technical and Organizational Measures) to this DPA; and

(iv) the list of Subprocessors is located in Schedule 1 (Subject Matter and Details of Processing) to this DPA.

(f) in Table 4 of the UK Addendum, both the Importer and the Exporter may end the UK Addendum in accordance with its terms (and the respective box for each is deemed checked); and

(g) in Part 2: Part 2 – Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with section 119 (A) of the Data Protection Act 2018 on 2 February 2022, as it is revised under section 18 of those Mandatory Clauses.

Schedule 4: Region-Specific Terms

A. CALIFORNIA

1. Definitions. CCPA and other capitalized terms not defined in this Schedule are defined in the DPA.

1.1. "business purpose", "commercial purpose", "personal information", "sell", "service provider" and "share" have the meanings given in the CCPA.

1.2. The definition of "Data Subject" includes "consumer" as defined under the CCPA.

1.3. The definition of "Controller" includes "business" as defined under the CCPA.

1.4. The definition of "Processor" includes "service provider" as defined under the CCPA.

2. Obligations.

2.1. Customer is providing the Customer Personal Data to Provider under the Agreement for the limited and specific business purposes of providing the Services as described in Schedule 1 (Subject Matter and Details of Processing) to this DPA and otherwise performing under the Agreement.

2.2. Provider will comply with its applicable obligations under the CCPA and provide the same level of privacy protection to Customer Personal Data as is required by the CCPA.

2.3. Provider acknowledges that Customer has the right to: (i) take reasonable and appropriate steps under Section 9. (Audits) of this DPA to help to ensure that Provider's use of Customer Personal Data is consistent with Customer's obligations under the CCPA, (ii) receive from Provider notice and assistance under Section 7. (Data Subject Requests) of this DPA regarding consumers' requests to exercise rights under the CCPA and (iii) upon notice, take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

2.4. Provider will notify Customer promptly after it makes a determination that it can no longer meet its obligations under the CCPA.

2.5. Provider will not retain, use or disclose Customer Personal Data: (i) for any purpose, including a commercial purpose, other than the business purposes described in Section 2.1. of this Section A (California) of Schedule 4 or (ii) outside of the direct business relationship between Provider with Customer, except, in either case, where and to the extent permitted by the CCPA.

2.6. Provider will not sell or share Customer Personal Data received under the Agreement.

2.7. Provider will not combine Customer Personal Data with other personal information except to the extent a service provider is permitted to do so by the CCPA.