Retell AI

Full Name: Eugen Regehr

Email: hello@maklervox.de

Company: MaklerVox

Job Title: CEO

Date: 7.5.2026

Data Processing Addendum

Last updated August 29, 2025

This Data Processing Addendum ("**DPA**") is an Attachment to the **Agreement**.and is between Retell AI, Inc., a Delaware corporation ("**Provider**"), and the customer named on any Order Form or in the DocuSign Click process that incorporates or is incorporated into this DPA, or any other person or entity whose use of the Services is not governed by a superseding agreement ("**Customer**"). By clicking to accept, signing an Order Form incorporating this DPA, making payment in accordance with such Order Form, or otherwise accessing or using Provider's Services, including Provider's websites, Customer agrees that Customer Personal Data processed in connection with the Services will be governed by this DPA. If you are accepting this DPA on behalf of a company or other legal entity, you represent and warrant that you have the authority to bind such entity (and its affiliates, as applicable) to this DPA.

1. Definitions.

1.1. "**Agreement**" means the Agreement between Customer and Provider (the SaaS Agreement).

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

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

1.4. "**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.

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

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

1.7. "**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 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.

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

1.9. "**DPA Effective Date**" is specified on the DPA Setup Page.

1.10. “**DPA Setup Page**” means a separate document executed by Customer and Provider which causes this DPA to become an Attachment to their Agreement. If the DPA is integrated into the Agreement, then this means the relevant sections of the Agreement.

1.11. “**EEA**” means European Economic Area.

1.12. “**Key Terms**” means Agreement, DPA Effective Date and Subprocessor List as specified by the parties on the DPA Setup Page.

1.13. “**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.

1.14. “**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.

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

1.16. “**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.

1.17. “**Schedules**” means one or more schedules incorporated by the parties in their DPA Setup Page. The default Schedules for this DPA 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

1.18. “**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.

1.19. “**Specified Notice Period**” is 48 hours.

1.20. “**Subprocessor**” means any third party authorized by Provider to Process any Customer Personal Data.

1.21. “**Subprocessor List**” means the list of Provider’s Subprocessors as identified here: https://trust.retellai.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. Except in connection with a Security Incident, Provider reserves the right to charge Customer for any excessive or non-standard assistance provided in connection with this DPA, including but not limited to support with audits, questionnaires, and/or Data Subject or other information requests, that materially exceeds the scope reasonably necessary for routine compliance with this DPA and Data Protection Laws. Such fees will be charged at Provider’s then-current rates, with prior written notice to Customer.

2.3. Duration of DPA. This DPA commences on the **DPA Effective Date** and 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), (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 the Cloud Service 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 (but 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 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 is responsible to (a) comply with (i) Data Protection Laws in its issuing of Customer Instructions to Provider and (ii) Security Incident notification laws in fulfilling any obligations to give notices to government authorities, affected individuals or others relating to any Security Incidents; (b) 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; and (c) review the information made available by Provider relating to data security and making an independent determination as to whether the Cloud Service meets Customer's requirements and legal obligations under Data Protection Laws.

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.

2 (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. Provider may update the **Subprocessor List** from time to time. At least 15 days before any new Subprocessor Processes any Customer Personal Data, Provider will add such Subprocessor to the **Subprocessor List.**

4.4. Objection Right. Customer may object in writing to Provider's appointment of a new Subprocessor within ten (10) days after notice, provided such objection is based on reasonable data protection grounds. In such event, the parties will work together in good faith to resolve the objection. If the parties are unable to reach a mutually agreeable resolution within a

reasonable time, Customer may terminate the this DPA by providing written notice to Provider, and Provider will refund Customer a pro-rated portion of any prepaid, unused fees as of the date of termination.

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 Measures 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, 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) Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including 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 Cloud Service 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 Cloud Service, 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 Cloud Service).

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 Cloud Service or such other means specified on the DPA Setup Page, access, return to itself or delete Customer Personal Data.

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 written confirmation of deletion upon Customer's 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. Third-Party Compliance Program.

(a) Provider will describe its 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 at reasonable intervals (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) Provider shall provide Customer with its current SOC 2 Type II report upon Customer's request, and such report shall serve as Customer's sole method of assessing Provider's data security controls in lieu of direct audit rights. However, if Provider fails to furnish an acceptable SOC 2 report within thirty (30) days of Customer's request, or if the provided report does not meet mutually agreed criteria for currency or adequacy to verify Provider's compliance with this DPA or the parties' compliance with Data Protection Laws, Customer shall then have the right, at Customer's expense, to conduct an audit, of reasonable scope and duration, of Provider's data processing operations pursuant to a mutually agreed-upon audit plan with Provider that is consistent with the Audit Parameters (an "**Audit**").

(b) Each Audit must conform to the following parameters ("**Audit Parameters**"): (i) be conducted by an independent third party that will enter into a confidentiality agreement with Provider, (ii) be limited in scope to matters reasonably required for Customer to assess Provider's compliance with this DPA and the parties' compliance with Data Protection Laws, (iii) occur at a mutually agreed date and time and only during Provider's regular business hours, (iv) occur no more than once annually (unless required under Data Protection Laws or in connection with a Security Incident), (v) cover only facilities controlled by Provider, (vi) restrict findings to systems that Process Customer Personal Data only (but such Audits will not involve or impact Personal Data that Provider Processes on behalf of other customers) and (vii) treat any results as confidential information to the fullest extent permitted by Data Protection Laws.

10. Liability.

10.1. Notwithstanding anything to the contrary in the Agreement or this DPA, each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or relating to this DPA, the Standard Contractual Clauses, and any other data protection agreements in connection with the Agreement (if any), shall be subject to any aggregate limitations on liability set out in the Agreement. Without limiting the parties' obligations under the Agreement, each party agrees that any regulatory penalties incurred by one party (the "**Incurring Party**") in relation to the Customer Personal Data that arise as a result of, or in connection with, the other party's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Incurring Party's liability under the Agreement as if it were liability to the other party under the Agreement.

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

11.1. Cross-Border Data Transfers.

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

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

11.2. 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.

Schedule 1: Subject Matter and Details of Processing

Customer / 'Data Exporter' Details

Name:	MaklerVox
Contact details for data protection:	Eugen Regehr , hello@maklervox.de
Main address:	
Customer activities:	
Role:	Controller
	Provider / 'Data Importer' Details
Name:	Retell AI, Inc.
Contact details for data protection:	Bing Wu, CEO, bing@retellai.com
Main address:	1121 Industrial Ave., Suite 500, San Carlos, CA 94070
Provider activities:	Providing the Services to Customer
Role:	Processor

Details of Processing

	Customer may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:
Categories of Data Subjects:	● Prospects, customers, business partners and vendors of Customer (who are natural persons)
	● Employees or contact persons of Customer's prospects, customers, business partners and vendors
	● Employees, agents, advisors, freelancers of Customer (who are natural persons)
	● Customer's users authorized by Customer to use the Services
	Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:
	● First and last name
Categories of Customer Personal	● Title
Data:	● Position
	● Employer
	● Contact information (company, email, phone, physical business address)
	● ID data

	● Professional life data
	● Localization data
Sensitive Categories of Data and additional associated restrictions/safeguards:	N/A
Frequency of transfer:	Continuous

Nature of the Processing:	Such processing as is necessary to enable Provider to comply with its obligations and exercise its rights under the Agreement, including on-demand conversational voice-to-text and text-to-voice interactions.
Purpose of the Processing:	Provider agrees to process Personal Data for limited and specified purposes (including services for conversational user interactions, including text and voice) described in the Agreement, this DPA, or as otherwise directed by authorized personnel of Customer in writing (email acceptable).
Duration of Processing / retention period:	Provider agrees to process Personal Data solely as instructed in the Agreement and the DPA for the duration of the provision of the Services to Customer, and the longer of such additional period as: (i) is specified in any provisions of the Agreement regarding data retention; and (ii) is required for compliance with law.
Transfers to Subprocessors:	Transfers to Subprocessors will occur where necessary for the provision of the Services in accordance with the Agreement and the DPA solely for the term of the Agreement.

Schedule 2: Technical and Organizational Measures

1. **Security Staffing.**

● Organizational management and dedicated staff responsible for the development, implementation and maintenance of Provider's information security program.

● Employees must complete management-approved security training during onboarding and revisit such training annually throughout their tenure.

2. **Audit and Risk Assessment.** Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Provider's organization, monitoring and maintaining compliance with Provider's policies and procedures, and reporting the condition of Provider's information security and compliance to internal management.

3. **Security Controls.** Data security controls which include, at a minimum:

● Logical segregation of data;

● Restricted (e.g., role-based) access and monitoring; and

● Utilization of encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest or stored on portable or removable media (i.e., laptop computers, CD/DVD, USB drives, back-up tapes).

4. **Access Controls.** Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur).

5. **Password Security.** Password controls designed to manage and control password strength, expiration and usage, including prohibiting users from sharing passwords and requiring that Provider's passwords that are assigned to its employees:

● Be at least eight (8) characters in length;

● Not be stored in readable format on Provider's computer systems; and

● Newly issued passwords must be changed after first use.

6. **System Event Logging.** System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. **Physical Security.** Physical and environmental security of areas containing Personal Data managed by Provider that are designed to:

● Protect information assets from unauthorized physical access;

● Manage, monitor and log movement of persons into and out of Provider's facilities; and

● Guard against environmental hazards such as heat, fire and water damage.

8. **Operational Procedures.** Operational procedures and controls designed to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of systems and media designed to render data contained therein as undecipherable or unrecoverable prior to final disposal or release from Provider's possession.

9. **Change Management.** Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to Provider's technology and information assets.

10. **Incident response.** Incident response management procedures designed to allow Provider to investigate, respond to, mitigate and notify of events related to Provider's technology and information assets.

11. **Network Security.** Network security controls that utilize firewalls and segregated access, and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12. **Vulnerability Management Processes.**

● Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code; and

● Third party vulnerability assessments are conducted periodically and vulnerabilities are remediated as appropriate in accordance with Provider's internal risk assessment policies.

13. **Business Continuity/Disaster Recovery.** Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergencies or disasters. Provider Business Continuity and Disaster Recovery procedures (including restoration from backups) are reviewed and tested annually.

14. **Policy Review.** Provider's security and privacy policies are reviewed and approved annually for Provider's business operations.

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 Standard Contractual Clauses approved by the European Commission in decision 2021/914.

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:	Ireland	
"**Designated EU Member State**" means:	Ireland	

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 2 (Controller to Processor) applies where Customer is a Controller of Customer Personal Data and Provider is a Processor of Customer Personal Data; (b) Module 3 (Processor to Processor) applies where Customer is a Processor of Customer Personal Data (on behalf of a third- party Controller) and Provider is a Processor of Customer Personal Data; (c) Customer is the "data exporter" and Provider 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, Option 1 will apply, and the EU SCCs will be governed by Designated EU Governing Law;

(f) in Clause 18(b), disputes will be resolved before the courts of the Designated EU Member State;

(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.

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 (Option 1), the EU SCCs will be governed by the laws of Switzerland;

(c) in Clause 18(b), 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.

5. Data Privacy Framework. For clarity, a transfer of Customer Personal Data from the EU, UK or Switzerland to Provider in the United States subject to the EU-U.S. Data Privacy Shield Framework, the UK Extension to the EU-U.S. Data Privacy Framework, and/or the Swiss-U.S. Data Privacy Shield Framework, as applicable (collectively, the "**DPF**"), shall not constitute a Restricted Transfer so long as Provider maintains an active certification to the DPF and certification to the DPF remains a legal basis for transfer of Personal Data to the United States under the GDPR, UK GDPR or FADP, as applicable.

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 Cloud Service 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.