VONAGE

Effective date July 06, 2022

DPA v3

This Data Processing Addendum ("**DPA**") is incorporated into the services agreement between the Vonage Group entity with whom the customer ("**Customer**") has entered into a services agreement ("**Agreement**") for one of the following service offerings:

- Communications APIs services, as described at https://www.vonage.com/communications-apis/ ("API Services");
- Unified Communications services, as described at https://www.vonage.com/unified-communications ("UC Services"); or
- Contact Center services, as described at https://www.vonage.com/contact-centers/ ("CC Services").
- Jumper.ai, a Vonage solution for Conversational Commerce Services, as described at https://www.vonage.co.uk/conversational-commerce/ ("Jumper.ai")

Herein, "Services" shall mean, with respect to the Agreement that this DPA is incorporated into, the API Services, UC Services, CC Services, and/or Jumper.ai provided pursuant to that Agreement, and "Vonage" shall mean the Vonage Group entity that is the service provider to Customer under such Agreement.

1. Definitions. All capitalized terms used but not otherwise defined in this DPA shall have the meaning ascribed to such terms in the Agreement. The following definitions and rules of interpretation below apply to this DPA:

"Adequate" in relation to the level of protection given to Personal Data in countries outside the European Economic Area ("EEA") or United Kingdom, means a decision made by the European Commission under Article 25(6) of Directive 95/46/EC (as amended or replaced from time to time) or Information Commissioner's Office, finding that the relevant third country provides an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.

"Applicable Data Protection Law(s)" refers to all laws and regulations applicable in relation to the processing of Personal Data under the Agreement.

"controller", **"processor"**, **"data subject"** and **"processing"** (and **"process"**) have the meanings given in accordance with Applicable Data Protection Law.

"Customer Account Data" means (a) Personal Data that relates to Customer's relationship with Vonage, including the names, phone numbers and/or contact information of individuals authorized by Customer to access Customer's Vonage account and/or use the Services and billing information; and (b) Personal Data processed by Vonage for the purposes of storing, transmitting or exchanging Customer Content, sending goods, and to provide the Services, that may include shipping address, data used to trace and identify the source and destination of a communication, such as individual data subjects' telephone numbers, data on the location of the device generated in the context of providing the Services, and the date, time, duration and type of communication, and/or data provided by the channels used by the Customer to communicate with their customers.

"Customer Content" means Personal Data exchanged by use of the Services, such as text, call recording, message bodies, conversation transcriptions, voicemail recordings, voicemail transcription, video recording, video files, images and sound.

"End User" means individuals or businesses who contact or are contacted by the Customer using the Services.

reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Security Incident" means a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to, Personal Data transmitted, stored or otherwise processed.

"Sensitive Personal Data" means Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or any other data that falls within the definition of "special categories of data" under Applicable Data Protection Law.

"Standard Contractual Clauses" or "SCC" means

(a) for the transfer of data from the EEA outside the EEA to a non-adequate country, the standard contractual clauses for the transfer of personal data to third countries approved by the European Commission in the decision (EU) 2021/914 of 4 June 2021 ("EEA SCCs")

(b) for the transfer of data from the United Kingdom to a non-adequate country, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022 (" UK International Data Transfer Addendum").

"Sub-processor" means any processor engaged by Vonage for the purposes of the provision of the Services under the Agreement.

"Vonage Group" means the corporate entities that from time-to-time control, are controlled by or are under common control with Vonage Holdings Corp.

2. Relationship of the Parties

2.1 Customer Content. The parties acknowledge and agree that with regard to the processing of Customer Content, Customer may act either as a controller or processor and Vonage acts as a processor (where Customer is a controller) or sub-processor (where Customer is a processor); and an independent data controller (and the Customer is a controller) for the purpose of improving and enhancing the Services.

2.2 Customer Account Data. The parties acknowledge that, with regard to the processing of Customer Account Data, Customer is a controller and Vonage is an independent controller, not a joint controller with Customer.

3. Processing of Personal Data

3.1 Purpose Limitation. Vonage shall process Customer Content as a data processor (a) for the performance of the Services in accordance with Customer's instructions as set forth in the Agreement and this DPA and in accordance with Applicable Data Protection Law, (b) as otherwise necessary to provide the Services (which may include responding to support requests and prevention and resolution of security, fraud and technical issues, the latter may include engaging and providing access to Customer Content to telecommunication carriers to diagnose and solve the issue), (c) as initiated through the use of the Service and (d) as further instructed by the Customer in writing. Vonage shall process Customer Content as a data controller to improve and enhance the Services. Vonage will process Customer Account Data as a data controller in accordance with Applicable Data Protection Law, the Privacy Policy[1] and the Agreement for the purposes detailed in Schedule 1 of this DPA.

3.2 Customer Instructions. Customer will ensure that its instructions comply with Applicable Data Protection Laws and that Vonage's processing of the Customer Content in accordance with Customer's instructions will not cause Vonage to violate Applicable Data Protection Laws. Vonage will notify Customer to the extent permitted by law if it becomes aware or reasonably believes that Customer's data processing instructions would violate Applicable Data Protection Law.

Vonage's processing activities for which Vonage acts as a controller, to fulfil the requirements of Applicable Data Protection Laws (c) it has, and will continue to have, the right to transfer, or provide access to, its customers' and end users' Personal Data (including, as applicable, Sensitive Personal Data) to Vonage for processing in accordance with the terms of the Agreement and this DPA; and (d) appropriate technical and organisational measures and suitable safeguards are in place before transmitting or processing Sensitive Personal Data, and/or before permitting Customer's end users to transmit or process any Sensitive Personal Data via the Services.

3.4 Processing Information. Schedule 1 of this DPA details the duration of processing, the nature and purpose of processing, the type of Personal Data and the categories of data subjects processed by Vonage.

4. Sub-processors

4.1 Sub-processors list and engagement. Customer acknowledges that Vonage engages Sub-processors in connection with the provision of the Services and Customer provides general consent for Vonage to appoint sub-processors, subject to this clause 4. The engagement by Vonage of any such Sub-processor shall be on written terms which impose upon the Sub-processor data protection obligations to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, including providing sufficient guarantees to implement appropriate technical and organizational measures. Vonage's up-to-date sub-processors list is set forth here[2] (the "**Sub-processors List**").

4.2 General Consent for Vonage Group Sub-processors. Customer grants a general authorisation to Vonage to appoint other entities of Vonage Group as Sub-processors, conditional on the requirements detailed in Section 4.1

4.3 Notification Mechanism. When a Sub-processor is replaced or a new one appointed, the Sub-processors List may be modified pursuant to a notification mechanism[3] ("**Notification Mechanism**"). Customer may subscribe to the Notification Mechanism and if Customer subscribes, Vonage will provide notification of any proposed use of a new or replacement Sub-processor, and, where commercially feasible, the notice shall be provided at least thirty days' prior to such change. Vonage's notification will be sent to the email address Customer provided when subscribing to the Notification Mechanism.

4.4 Objection to new Sub-processors. If Customer objects to Vonage's appointment or replacement of a Sub-processor based on reasonable grounds relating to data protection, it shall notify Vonage in writing of such objection prior to the appointment or replacement of the Sub-processor. In such event, Vonage will use reasonable efforts to provide the Services to Customer in accordance with the Agreement without using the Sub-processor. If Vonage reasonably requires use of the Sub-processor and is unable to satisfy Customer as to the suitability of the Sub-processor within thirty (30) days of Customer's objection, the Customer may elect to terminate only the part of the Services or Order(s) which cannot be provided by Vonage without the use of the objected-to Sub-processor.

4.5 Sub-Processor liability. Vonage shall be liable for its Sub-processors' processing of Customer Content to the same extent that Vonage would be liable if performing the processing activities of each Sub-processor directly under the terms of this DPA.

4.6 Communications sent through the Services and payment gateways. Customer acknowledges that Vonage may use telecommunication providers in the provision of the Services. Customer further acknowledges that in order to send communications for the provision of the Services, Vonage may need to transmit Customer's communications through existing telecommunications networks and suppliers, via companies bound to comply with applicable telecommunications and privacy laws but who may not all have direct contracts with Vonage and/or Customer. Customer further acknowledges that Vonage may use payment gateways in the provision of Jumper.ai Services via companies bound to comply with data protection laws but who may not have direct contracts with Vonage. Customer hereby instructs Vonage to transmit the communications through existing telecommunications networks and to use payment gateways as necessary to provide the Services and acknowledges and agrees that telecommunications networks and payment gateways suppliers are not considered Sub-processors under either the DPA or the Agreement.

4.7 Call quality. When Customer reports potential issues with the quality of the Services, the Customer instructs Vonage to engage its relevant telecommunication suppliers for assistance including by providing them with

5. Data Transfers

5.1 Vonage data transfer. To the extent that any Personal Data is transferred from the European Economic Area, the United Kingdom, and/or Switzerland (either directly or via onward transfer) to any country that, according to the European Commission or the competent authority for the UK and Switzerland, does not provide an adequate level of protection for personal data, the parties agree that the Standard Contractual Clauses, incorporated by reference to this DPA, will apply in respect of the processing of such Personal Data. The Standard Contractual Clauses and this Clause 5 will not apply to Personal Data that is not transferred, either directly or via onward transfer, outside the EEA, the United Kingdom and/or Switzerland. In relation to the Standard Contractual Clauses, Vonage will comply with the obligations of the 'data importer' in the Standard Contractual Clauses and the Customer will comply with the obligations of the 'data exporter'. Appendices of the EEA SCCs shall be deemed completed as set forth in Schedule 2 of this DPA in relation to transfer of personal data outside the EEA. The UK International Data Transfer Addendum, applicable to transfer of personal data outside the United Kingdom, shall be deemed completed as set forth in Schedule 3.

5.2 In the event of any conflict or inconsistency between the EU Standard Contractual Clauses (Schedule 2) or UK International Data Transfer Addendum (Schedule 3), and the terms of this DPA, the EU Standard Contractual Clauses or UK International Data Transfer Addendum (Schedule 3), as applicable, shall prevail.

5.3 Request for Personal Data.

5.3.1 If Vonage receives a civil or criminal subpoena, search warrant, or other official and written request that is legally binding ("Request") by a public authority that is not from an EEA country, the UK, or a country considered Adequate ("Requesting Party") for disclosure of Customer's personal data, Vonage will, insofar as legally permissible, redirect the Requesting Party to request that Personal Data directly from Customer instead. If this is not possible, Vonage will promptly notify Customer about the Request to allow Customer to seek a protective order or other appropriate remedy if not precluded from doing so by the Request.

5.3.2 Vonage will review the Request to determine whether the Request is valid and if Vonage has a legal requirement to disclose Personal Data. Vonage will reject or contest any request that is not valid, legally binding and lawful. Vonage will also challenge any overbroad or inappropriate Requests or Requests that are otherwise subject to appropriate grounds for challenge.

5.3.3 In the event that the information must be provided, Vonage will (a) ensure that the disclosed Personal Data is the minimum required to satisfy the Request; and (b) take all commercially reasonable steps to ensure that such Customer information is afforded confidential treatment by the authorities.

5.4 Sub-processors data transfer. If in the performance of the Services, Vonage permits processing of any Personal Data by a Sub-processor outside the EEA, except if in an Adequate country, without prejudice to Section 4, Vonage shall in advance of any such transfer ensure that a legal mechanism to achieve adequacy in respect of that processing is in place, such as:

5.4.1 Standard Contractual Clauses; or

5.4.2 the existence of any other specifically approved safeguard for data transfers as recognised under Applicable Data Protection Law and/or a European Commission or Information Commissioner's Office finding of adequacy.

6. Security of Personal Data

6.1 Security measures. Vonage has implemented and will maintain appropriate administrative, technical, and organizational measures[4] to protect Personal Data from a Security Incident, having regard to the state of technological development and the cost of implementing such measures, as well as the nature, scope, context and purposes of processing and the likelihood and severity of harm to the interests of data subjects that may be expected to result from any such Security Incident.

6.2 Employee Access. Vonage shall ensure that only such of its employees who may be required by it to provide the Services to Customer or assist Vonage in meeting its obligations under this DPA shall have access to

7. Security Incidents

7.1 Security Incident Involving personal data. Upon confirming a Security Incident involving personal data for which Vonage acts a data processor, Vonage will:

7.1.1 to the extent permitted by applicable law, notify Customer without undue delay, such notice to be delivered in accordance with Section 13 of this DPA;

7.1.2 to the extent such Security Incident is caused by Vonage's violation of its obligations under this DPA, take such reasonable remedial steps to address such Security Incident and prevent any further incidents; and

7.1.3 promptly provide the Customer with all relevant information in its possession as reasonably required by Applicable Data Protection Law to comply with any reporting obligations of a relevant regulatory authority concerning such Security Incident.

7.2 Notification to the supervisory authority: If Customer determines that a Security Incident must be notified to any supervisory authority and/or data subjects and/or the public or portions of the public pursuant to the Applicable Data Protection Law, Customer will to the extent commercially feasible notify Vonage before the communication is made (and where not commercially feasible, as soon as is commercially feasible after such communication) and supply Vonage with copies of any written documentation to be filed with the supervisory authority and of any notification Customer proposes to make (whether to any supervisory authority, data subjects, the public or portions of the public) which directly or indirectly references Vonage, its security measures and/or role in the Security Incident, whether or not by name. Subject to Customer's compliance with any mandatory notification deadlines under Applicable Data Protection Law, Customer will consult with Vonage in good faith and take account of any clarifications or corrections Vonage reasonably requests to such notifications and which are consistent with Applicable Data Protection Law.

8. Audits

8.1 Demonstrated Compliance. Upon Customer's written request, no more than once annually and subject to adequate confidentiality provisions, Vonage shall, in accordance with Applicable Data Protection Laws, make available to Customer such reasonable information in Vonage's possession or control to demonstrate Vonage's compliance with its obligations as a data processor of Customer Content to satisfy Customer's audit rights granted by Applicable Data Protection Law (including, where applicable, the Standard Contractual Clauses).

9. Personal Data on Expiry or Termination

9.1 Deletion of Personal Data. In respect of the Customer Content that Vonage processes as data processor pursuant to the Agreement, Vonage shall cease to process such personal data and will promptly arrange for its deletion on expiry or termination of the Agreement, unless otherwise agreed by the parties in writing, in which case Vonage shall hold Customer Content in accordance with the data retention term agreed by the parties. Notwithstanding anything to the contrary in this Section 9, Vonage may retain Customer Content or any portion of it if required by applicable law, in which case, Vonage shall comply with Applicable Data Protection Law regarding the deletion and retention of Personal Data.

10. Data Protection Impact Assessment

10.1 Vonage shall provide reasonable assistance to Customer (taking into account the nature of processing and the information available to Vonage and at Customer's expense) with respect to data protection impact assessments or consultations with supervisory authorities that may be required in accordance with Applicable Data Protection Law.

11. Data Subject Request

11.1 Self-service features. As part of certain Services, Vonage may provide Customer with self-service features to delete, retrieve or restrict use of Customer Content, which the Customer may use to comply with its obligations

12.1 Additional assistance. In addition, upon request, Vonage will provide reasonable additional and timely assistance in relation to Customer Content, at Customer's expense, to assist Customer in complying with its data protection obligations to respond to requests for exercising the rights of data subject under Applicable Data Protection Law.

12. Liability

12.1 Liability. This DPA is without prejudice to the rights and obligations of the parties under the Agreement which shall continue to have full force and effect, including any limitations and exclusions on liability contained therein which shall apply to this DPA as if fully set forth herein. In the event of any conflict between the terms of this DPA and the terms of the Agreement, the terms of this DPA shall prevail so far as the subject matter concerns the processing of Personal Data.

12.2 Penalties. Notwithstanding anything to the contrary in this DPA or in the Agreement, neither party will be responsible for any fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party's violation of the GDPR.

13. Notification

13.1 All notices given by Vonage to Customer under or in connection with this DPA shall be validly served by email. Where Customer has subscribed to the Notification Mechanism, Customer shall receive notifications pursuant to Clause 4.3 of this DPA. All other notices given by Vonage to Customer under or in connection with this DPA shall be sent to Customer's email address associated to their Vonage account or as stated on the last Order executed by Customer; and any notice given by Customer to Vonage shall be sent to privacy@vonage.com.

14. Miscellaneous

14.1 Governing Law and Jurisdiction. This DPA shall be governed by and construed in accordance with the law and the jurisdiction of the country or territory which governs the Agreement, except as otherwise specified in this DPA, including its Schedules, or required by Applicable Data Protection Law.

14.2 Jurisdiction Specific Terms. To the extent Vonage processes Personal Data protected by Applicable Data Protection Laws in a jurisdiction listed in Schedule 4, then the terms specified in Schedule 4 ("**Jurisdiction Specific Terms**") apply and in case of any conflict between the Jurisdiction Specific Terms and any term of this DPA, the applicable Jurisdiction Specific Terms will take precedence.

14.3 Updates. Vonage may update the terms of this DPA where the changes (a) are required to comply with Applicable Data Protection Law, applicable regulation, a court order or guidance issued by a regulator or agency; or (b) do not have a material adverse impact on Customer's rights under the DPA. Vonage shall provide 30 days' notice prior to making any material change to the provisions of this DPA. If the Customer objects, the Customer has the right to terminate the affected Services within 30 days of receiving written notice of the changes.

---

[1] https://www.vonage.com/legal/privacy-policy/

[2] https://www.vonage.com/legal/subprocessors/

[3] https://www.vonage.com/legal/subprocessors/notification-mechanism

[4] https://www.vonage.com/legal/technical-organizational-security-practices/

Schedule 1

DETAILS OF PROCESSING

1. Nature and Purpose of processing

1.1 Customer Content. Vonage will process Customer Content in accordance with Section 3.1 of this DPA.

1.2 Customer Account Data. Vonage will process Customer Account Data as a controller to perform the functions as a communications service provider that may include, but are not limited to, (a) manage the relationship with the Customer; (b) carry out Vonage's business operations, such as accounting, tax, billing, audit and compliance; (c) to investigate security issues, fraud, unauthorised or unlawful use of the service and other misuses; (d) to improve the Services; and (e) as required by Applicable Data Protection Law.

2. Duration of Processing

2.1 Vonage acting as processor for Customer Content. Vonage will process Customer Content for the duration outlined in Section 9 of this DPA.

2.2 Vonage acting as controller. Vonage will process personal data as a controller for as long as needed to provide the Services. Upon termination of the Agreement, Vonage may retain personal data (a) for the purposes outlined in Section 1.2 of this Schedule 1; or (b) as required by law. Vonage will promptly delete or anonymize such personal data when Vonage no longer requires it for the herein mentioned purposes.

3. Types of Personal Data

3.1 Vonage processes personal data contained in Customer Content and Customer Account Data as defined in Section 1 of this DPA.

4. Categories of Data Subjects

4.1 Customer Content. Customer Content may concern the following categories of data subjects:

- Customer's authorized users, who are those individuals that are authorized by the Customer to use the Services on behalf of the Customer.
- Customer's customers and end users

4.2 Customer Account Data. Customer Account Data may concern the following categories of data subjects:

- Customer's employees and agents
- Customer's authorized users
- Customer's customers and end users

Schedule 2

STANDARD CONTRACTUAL CLAUSES Decision (EU) 2021/914

Terms applicable to the EEA SCCs

(ii) Clause 9 - Option 2 will apply and the time period for prior notice of sub-processor changes will be as set forth in Section 4 (Sub-processors) of this DPA;

(iii) Clause 11 (a) - the optional language will not apply;

(iv) Clause 17 - Option 1 will apply and the Clauses will be governed by the law of the Netherlands;

(v) Clause 18 - disputes will be resolved before the courts of the Netherlands;

(vi) Module One (Controller to Controller) of the EEA SCCs apply where Customer is a controller and Vonage is an independent controller

(vii) Module Two (Controller to Processor) of the EEA SCCs apply where Customer is a controller and Vonage is a processor

(viii) Module Three (Processor to Processor) of the EEA SCCs apply where Customer is a processor and Vonage is a processor

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

1. *Name:* The company defined as Customer who is party to the Agreement.

Address: The address of the Customer as provided in the Agreement.

Contact details: Customer's email address associated to their Vonage account or as stated on the last Order executed by Customer.

Activities relevant to the data transferred under these Clauses: purchase of Vonage Services.

Signature and date: By entering into the Agreement, Data Exporter is deemed to have signed these Standard Contractual Clauses, including their Annexes, as of the date the parties entered into the Agreement or this DPA, whichever is later.

Role: The Data Exporter's role is as set forth in Section 2 (Relationship of the Parties) of this DPA.

Data importer(s):

1. *Name:* The Vonage Group entity that is the service provider to Customer under the Agreement.

Address: The Vonage Group entity's address specified in the Agreement.

Contact details: Vonage Privacy Team, privacy@vonage.com

Activities relevant to the data transferred under these Clauses: Provision of Communications APIs services, Unified Communications services and/or Contact Centre services.

Signature and date: By entering into the Agreement, Data Importer is deemed to have signed the Standard Contractual Clauses, including their Annexes, as of the date the parties entered into the Agreement or this DPA, whichever is later.

Role: The Data Importer's role is as set forth in Section 2 (Relationship of the Parties) of this DPA.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred: As described in Section 4 of Schedule 1 (Details of Processing) of this DPA.

Categories of personal data transferred: Vonage processes personal data contained in Customer Content and Customer Account Data as defined in Section 1 (Definitions) of this DPA.

Sensitive data: N/A

The frequency of the transfer: The data is transferred on a continuous basis.

Nature of the processing: is as Section 1 of Schedule 1 (Details of Processing) of this DPA.

Purpose(s) of the data transfer and further processing: Vonage processes personal data for the purposes described in Section 1 of Schedule 1 (Details of Processing) of this DPA.

Sub-processors List (refer to Section 4.1 of this DPA).

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies: The Dutch supervisory authority is the competent supervisory authority.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational security measures implemented by the data importer are as set forth in Section 6.1 of this DPA. The data importer may update its security document from time to time provided that there is no degradation to the security and/or privacy of the services.

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

As per the Sub-processors List (in Section 4.1 of this DPA).

Schedule 3

UK International Data Transfer Addendum

Standard Data Protection International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018

VERSION B1.0, in force 21 March 2022

PART 1: Tables

Table 1: Parties

Start date	As set forth in the order or Agreement that incorporates these Standard Contractual Clauses by reference or as set forth in the DPA, whichever is later.

The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	*Full legal name:* The company defined as Customer who is party to the Agreement. *Trading name (if different):* *Main address (if a company registered address):* The address of the Customer as provided in the Agreement or order form. *Official registration number (if any) (company number or similar identifier):* As provided in the Agreement or order form.	*Full legal name: The* Vonage Group entity that is the service provider to Customer under the Agreement. *Trading name (if different):* *Main address (if a company registered address):* The Vonage Group entity address specified in the Agreement or order form. *Official registration number (if any) (company number or similar identifier):* as provided in the Agreement or order form.
Key Contact	*Full Name (optional):* *Job Title:*	*Full Name (optional):* *Job Title:*

	Customer	
Signature (if require for the purpose of Section 2)	By entering into the order form or the Agreement, the parties are deemed to have signed this UK International Data Transfer Addendum	By entering into the order form or the Agreement, the parties are deemed to have signed this UK International Data Transfer Addendum

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs: The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:

Date: as provided in Table 1 above

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)
1	Yes	Does not apply	Optional language does not apply		
2	Yes	Does not apply	Optional language does not apply	Option 2 applies - general authorization	At least thirty days' prior to such change, where commercially feasible. In any event no less than 10 days.
3	Yes	Does not apply	Optional language does not apply	Option 2 applies - general authorization	At least thirty days' prior to such change, where commercially feasible. In any event no less than 10 days.
4					

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: as set forth in Annex I.A of Schedule 2 of this DPA.

Annex 1B: Description of Transfer: as set forth in Annex I.B of Schedule 2 of this DPA.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: as set forth in Annex II of Schedule 2 of this DPA.

Annex III: List of Sub processors (Modules 2 and 3 only): as set forth in Annex II of Schedule 2 of this DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

PART 2: Mandatory Clauses

Mandatory Clauses:

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 s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Schedule 4

JURISDICTION SPECIFIC TERMS

Australia:

- The definition of "Applicable Data Protection Law" includes the Australian Privacy Principles (APPs) and the Australian Privacy Act (1988).
- The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Law.
- The definition of "sensitive data" includes "Sensitive Information" as defined under Applicable Data Protection Law.

Brazil:

- The definition of "Applicable Data Protection Law" includes the Lei Geral de Proteção de Dados (LGPD).
- The definition of "processor" includes "operator" as defined under Applicable Data Protection Law.
- The definition of "Security Incident" includes a security incident that may result in any relevant risk or damage to the data subjects.

California:

- The definition of "Applicable Data Protection Law" includes the California Consumer Privacy Act (CCPA).
- The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Law.
- The definition of "data subject" includes "Consumer" as defined under Applicable Data Protection Law. Any Data Subject Rights, as described in Section 11 of the DPA, apply to Consumer rights. In regards to Data Subject Requests, Vonage can only verify a request from Customer and not from Customer's end user or any third party.
- The definition of "controller" includes "Business" as defined under Applicable Data Protection Law.
- The definition of "processor" includes "Service Provider" as defined under Applicable Data Protection Law.
- Vonage will process, retain, use, and disclose Personal Data only as necessary to provide the Services under the Agreement, which constitutes a business purpose. Vonage agrees not to sell Customer's Personal Data or Customer end users' Personal Data; retain, use, or disclose Customer's Personal Data for any commercial purpose other than providing the Services; or retain, use, or disclose Customer's Personal Data

Applicable Data Protection Law, with whom Vonage has entered into a written contract that includes terms substantially similar to this DPA. Vonage conducts appropriate due diligence on its Sub-processors.

- Vonage will implement and maintain the reasonable security procedures and practices appropriate to the nature of the Personal Data it processes as set forth in Section 6 of the DPA.

Canada:

- The definition of "Applicable Data Protection Law" includes the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).
- Vonage's Sub-processors, as described in Section 4 of the DPA, are third parties under Applicable Data Protection Law, with whom Vonage has entered into a written contract that includes terms substantially similar to this DPA. Vonage has conducted appropriate due diligence on its Sub-processors.
- Vonage will implement technical and organizational measures as set forth in Section 6 of the DPA.

European Union:

- The definition of "Applicable Data Protection Law" includes the EU General Data Protection Regulation (Regulation 2016/679) ("GDPR").

Israel:

- The definition of "Applicable Data Protection Law" includes the Protection of Privacy Law (PPL).
- The definition of "controller" includes "Database Owner" as defined under Applicable Data Protection Law.
- The definition of "processor" includes "Holder" as defined under Applicable Data Protection Law.
- Vonage will require that any personnel authorized to process Customer Content comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Law. Such personnel sign confidentiality agreements with Vonage in accordance with Section 6 of the DPA.
- Vonage must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Section 6 of the DPA and complying with the terms of the Agreement.
- Vonage must ensure that the Personal Data will not be transferred to a Sub-processor unless such Sub-processor has executed an agreement with Vonage pursuant to Section 4.1 of this DPA.

Japan:

- The definition of "Applicable Data Protection Law" includes the Act on the Protection of Personal Information (APPI).
- The definition of "Personal Data" includes "Personal Information" as defined under Applicable Data Protection Law.
- The definition of "controller" includes "Business Operator" as defined under Applicable Data Protection Law. As a Business Operator, Vonage is responsible for the handling of Personal Data in its possession.

Singapore:

- The definition of "Applicable Data Protection Law" includes the Personal Data Protection Act 2012 (PDPA).
- Vonage will process Personal Data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Section 6 of the DPA and complying with the terms of the Agreement.

United Kingdom:

VONAGE

United Kingdom, this is UK GDPR and Data Protection Act 2018).

9/22/2022, 2:00:54 PM

DocuSigned by:
Emmy Hackett
F824F46BEA71411...

01 December 2022

Emmy Hackett

General Counsel