Vortexa Data Processing Addendum
(version 1.2, May 2024)

This Data Processing Addendum ("DPA") is an addendum to the Vortexa Master Subscription Agreement (the "Agreement"), between the Vortexa entity that agreed the same ("Vortexa") and the customer who has subscribed to the Vortexa Service as defined in the Agreement ("Customer"), and will be incorporated by reference into, and subject to the terms and conditions of, the Agreement. In the event of any inconsistency or conflict between this DPA and the Agreement with respect to the Processing of Customer Personal Data, the terms of this DPA will govern solely to the extent of such inconsistency or conflict.

This DPA sets out the terms that apply when Customer Personal Data is Processed by Vortexa under the Agreement. The purpose of the DPA is to ensure such Processing is conducted in accordance with the Data Protection Legislation and respects the rights of individuals whose Personal Data is Processed under the Agreement. This DPA applies to Vortexa and any Vortexa affiliate involved in the Processing of Customer Personal Data.

1. Definitions.

In this DPA, all of the definitions stated in the Agreement shall apply herein and in addition:

1.1. "Controller" means "Controller" or "Business" as those terms are defined by applicable Data Protection Legislation.

1.2. "Customer Personal Data" means Personal Data that Vortexa collects to administer the Service.

1.3. "Data Privacy Framework" means the EU-US Data Privacy Framework, the Swiss-US Data Privacy Framework, and the UK Extension to the EU-US Data Privacy Framework self-certification programs (as applicable) operated by the U.S. Department of Commerce, as may be amended, superseded, or replaced from time to time.

1.4. "Data Privacy Framework Principles" means the Data Privacy Framework Principles and Supplemental Principles contained in the relevant Data Privacy Framework, as may be amended, superseded, or replaced from time to time.

1.5. "Data Protection Legislation" means privacy and data protection laws and regulations applicable to Vortexa's Processing of Customer Personal Data in the provision of the Service to Customer, including, as applicable: (a) the GDPR; (b) any legislation which implements or supplements the GDPR; (c) any legislation which implements the European Community's Directive 2002/58/EC; (d) in respect of the United Kingdom, the Data Protection Act 2018 and the EU GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018; (e) the Federal Data Protection Act of 19 June 1992 (Switzerland) and its implementing regulations; (f) U.S. Privacy Laws; and/or (g) The Personal Data Protection Act ("The PDPA") in Singapore; in each case, as may be amended, superseded, or replaced from time to time.

1.6. "Data Subject" means an individual to whom Customer Personal Data relates.

1.7. "GDPR" means the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the Processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, and any amendment or replacement to it.

1.8. "Personal Data" means any data or information that constitutes "personal data," "personal information," or any analogous term as defined by applicable Data Protection Legislation.

1.9. "Process," "Processing," and "Processed" have the meaning as defined by applicable Data Protection Legislation.

1.10. "Processor" means "Processor," "Service Provider," or "Contractor" as those terms are defined by applicable Data Protection Legislation.

1.11. "Sale" and "Selling" have the meaning defined in U.S. Privacy Laws.

1.12. "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise Processed.

1.13. "Standard Contractual Clauses" or "SCCs" means the clauses annexed to the EU Commission Implementing Decision 2021/914 of June 4, 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 as amended or replaced from time to time, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN.

1.14. “Supervisory Authority” will have the meaning ascribed to it in the GDPR.

1.15. “UK Addendum” means the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).

1.16. “U.S. Privacy Laws” means U.S. privacy and data protection laws and regulations applicable to Vortexa’s Processing of Customer Personal Data in the provision of the Service to Customer, including, as applicable, (a) the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended by the California Privacy Rights Act, and its implementing regulations (“CCPA”); (b) Colorado Privacy Act, Colorado Rev. Stat. §§ 6-1-1301 to 6-1-1313; (c) Connecticut Personal Data Privacy and Online Monitoring Act, Public Act No. 22-15); (d) Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 to 13-61-404); and (e) Virginia Consumer Data Protection Act, Virginia Code Ann. §§ 59.1-575 to 59.1-585.

1.17. “Vortexa” means Vortexa Inc., Vortexa Ltd or Vortexa Asia Pte Ltd as stated on the Agreement.

1.17. The terms “Business,” “Share,” and “Service Provider” as used in this DPA will have the meanings ascribed to them in the CCPA.

2. Processing of Data

2.1. *Scope and Purpose of Processing.* This DPA applies only where and to the extent Data Protection Legislation governs Vortexa’s Processing of Customer Personal Data on behalf of Customer in the course of providing the Service pursuant to the Agreement, including Vortexa’s Processing of Customer Personal Data for the nature, purposes, and duration set forth in Appendix I. Vortexa will not collect, use, disclose, release, disseminate, transfer, or otherwise communicate or make available to a third-party Customer Personal Data except to provide the Service or as expressly permitted by the Agreement or this DPA.

2.2. *Processor and Controller Responsibilities.* The parties acknowledge and agree that: (a) Vortexa is a Processor of Customer Personal Data under the Data Protection Legislation; (b) Customer is a Controller or Processor, as applicable, of Customer Personal Data under the Data Protection Legislation; and (c) each party will comply with the obligations applicable to it under the Data Protection Legislation regarding the Processing of Customer Personal Data.

2.3. *Authorization by Third-Party Controller.* If Customer is a Processor, Customer warrants to Vortexa that Customer’s instructions and actions with respect to Customer Personal Data, including its appointment of Vortexa as another Processor, have been authorized by the relevant Controller.

2.4. *Customer Instructions.* Customer instructs Vortexa to Process Customer Personal Data: (a) in accordance with the Agreement, this DPA, any applicable order, and Customer’s use of the Service; and (b) to comply with other reasonable instructions provided by Customer or a user where such instructions are consistent with the terms of the Agreement. Customer will ensure that its instructions for the Processing of Customer Personal Data comply with the Data Protection Legislation. Customer has sole responsibility for the accuracy, quality, and legality of Customer Personal Data and the means by which Customer obtained the Customer Personal Data. Customer will disclose Customer Personal Data to Vortexa solely pursuant to a valid business purpose.

2.5. *Vortexa’s Compliance with Customer Instructions*. Vortexa will only Process Customer Personal Data in accordance with Customer’s instructions and will treat Customer Personal Data as Confidential Information. Vortexa may Process Customer Personal Data other than on the written instructions of Customer if it is required under applicable law to which Vortexa is subject. In this situation, Vortexa will inform Customer of such requirement before Vortexa Processes the Customer Personal Data unless prohibited by applicable law.

2.6. *Assistance with Customer’s Obligations*. Customer may request Vortexa to, correct, amend, restrict, block or delete Customer Personal Data contained in the Service. Vortexa will promptly comply with reasonable requests by Customer to assist with such actions to the extent Vortexa is legally permitted and able to do so. Vortexa may charge a reasonable fee for any assistance not strictly required by Data Protection Legislation.

2.7. *Notification Obligations*. Vortexa will, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject for access to, correction, amendment, deletion of or objection to the Processing of Customer Personal Data relating to such individual. Vortexa will forward such Data Subject request relating to Customer Personal Data to Customer and Customer will be responsible for responding to any such request. Vortexa will provide Customer with commercially reasonable cooperation and assistance in relation to handling of a Data Subject request, to the extent legally permitted and to the extent Customer does not have access to such Customer Personal Data through its use or receipt of the Service.

2.8. *General Authorization for Subprocessors*. Customer generally authorizes the use of subprocessors to process Customer Personal Data in connection with fulfilling Vortexa's obligations under the Agreement and/or this DPA and explicitly approves the list of subprocessors located at www.vortexa.com/sub-processors/.

2.9. New Subprocessors. When Vortexa engages a new subprocessor to Process Customer Personal Data, Vortexa will, at least thirty (30) days before the new subprocessor Processes any Customer Personal Data, notify Customer and give Customer the opportunity to object to such subprocessor. If Customer has reasonable grounds to object to Vortexa's change in subprocessors related to data protection concerns, Customer shall notify Vortexa promptly within no more than thirty (30) days after receipt of Vortexa's notice. Vortexa will use reasonable efforts find an acceptable, reasonable, alternate solution; otherwise, Customer may suspend or terminate the Service. If Customer terminates, Vortexa will promptly refund any fees paid in advance by Customer to Vortexa pro rata.

2.10. *Vortexa Obligations.* Vortexa will remain liable for the acts and omissions of its subprocessors to the same extent Vortexa would be liable if performing the service provided by the subprocessor directly. Vortexa will contractually impose data protection obligations on its subprocessors that are at least equivalent to those data protection obligations imposed on Vortexa under this DPA.

2.12. *Audit Rights*. Upon Customer's written request by email to dpo@vortexa.com no more than once per year, Vortexa will provide a copy of any recent third-party audits or certifications, as applicable, or any summaries thereof, such that Customer may reasonably verify Vortexa's compliance with the technical and organizational measures required under this DPA. Where required by the applicable Data Protection Legislation, Vortexa will allow Customer or a mutually agreed upon independent auditor appointed by Customer to conduct an audit to verify compliance with this DPA (including inspection), no more than once per year upon eight weeks' notice sent to dpo@vortexa.com complete with a detailed audit plan describing the proposed scope, duration, and start date of the audit. Vortexa will contribute to such audits whose sole purpose will be to verify Vortexa's compliance with its obligations under this DPA. The auditor must execute a written confidentiality agreement reasonably acceptable to Vortexa before conducting the audit. The audit must be conducted during Vortexa's normal business hours, subject to Vortexa's policies, and may not unreasonably interfere with Vortexa's business activities. Any audits are at Customer's sole cost and expense and the results shall be shared only with Vortexa and no other third party.

2.13. *Separate Service*. Any request for Vortexa to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required by law. Customer will reimburse Vortexa for any time spent for such separate services for any such audit at reasonable rates mutually agreed to by the parties, taking into account the resources expended by Vortexa. Customer will promptly notify Vortexa with information regarding any non-compliance discovered during the course of an audit.

2.14. *Limits on Auditing Party*. Nothing in this DPA will require Vortexa to disclose to an independent auditor or Customer, or to allow an independent auditor or Customer to access: (a) any data of any other user or customer of Vortexa; (b) Vortexa's internal accounting or financial information; (c) any trade secret of Vortexa; (d) any premises or equipment not controlled by Vortexa; or (e) any information that, in Vortexa's reasonable opinion, could: (i) compromise the security of Vortexa's systems or premises; (ii) cause Vortexa to breach its obligations under Data Protection Legislation or the rights of any third-party; or (iii) any information that an independent auditor seeks to access for any reason other than the good faith fulfilment of Customer's rights under the Data Protection Legislation. Customer will contractually impose, and designate Vortexa as a third-party beneficiary of, any contractual terms that prohibit any independent auditor from disclosing the existence, nature, or results of any audit to any party other than Customer unless such disclosure is required by applicable law.

3. **GDPR**

3.1. *Applicability*. Section 3 only applies to Vortexa's Processing of Customer Personal Data subject to GDPR.

3.2. *Data Privacy Impact Assessments*. Vortexa will take reasonable measures to cooperate and assist Customer in conducting a data protection impact assessment and related consultations with any Supervisory Authority, if Customer is required to do so under Data Protection Legislation.

3.3. *International Transfers.* The parties will transfer Customer Personal Data internationally only pursuant to a transfer mechanism valid under the Data Protection Legislation or applicable law, i.e. a valid mechanism in the exporting country. For example, in the case of transfers from within the European Economic Area or the United Kingdom to another country,

a scheme which is approved by the European Commission or the UK Government as ensuring an adequate level of protection or any transfer which falls within a permitted derogation.

3.4. *Transfer Mechanism*. In the event there is more than one mechanism to transfer Customer Personal Data from the European Economic Area, United Kingdom, and/or Switzerland to countries which do not ensure an adequate level of data protection under the Data Protection Legislation, the transfer of Customer Personal Data will be subject to a single transfer mechanism in the following order of precedence: (a) the Data Privacy Framework; (b) a valid transfer mechanism approved for transfers of Customer Personal Data from the European Economic Area, United Kingdom, or Switzerland to the U.S.; or (c) the SCCs and/or the UK Addendum, each as applicable.

3.6. *European Economic Area Data Transfers:* If applicable based on Section 3.4, Vortexa and Customer conclude Module 2 (Controller-to-Processor) of the SCCs and, to the extent Customer is a Processor on behalf of a third-party Controller, Module 3 (Processor-to-Subprocessor) of the SCCs, which are hereby incorporated and completed as follows: the "data exporter" is Customer; the "data importer" is Vortexa; the optional docking clause in Clause 7 is implemented; Option 2 of Clause 9(a) is implemented and the time period therein is specified in Section 2 of this DPA; the optional redress clause in Clause 11(a) is struck; Option 1 in Clause 17 is implemented and the governing law is the law of Ireland; the courts in Clause 18(b) are the courts of Dublin, Ireland; Annex I, II and III to the SCCs are Annex I, II and III to this DPA respectively.

3.7. *UK Data Transfers*: If applicable based on Section 3.4, Vortexa and Customer conclude the UK Addendum, which is hereby incorporated and applies to Customer Personal Data transfers outside the UK. Part 1 of the UK Addendum is completed as follows: in Table 1, the "Exporter" is Customer and the "Importer" is Vortexa, their details are set forth in this DPA and the Agreement; in Table 2, the first option is selected and the "Approved EU SCCs" are the SCCs; in Table 3, Annexes 1 (A and B) to the "Approved EU SCCs" are Annex I, II and III to this DPA respectively; and in Table 4, both the "Importer" and the "Exporter" can terminate the UK Addendum.

3.8. *Changes to Transfer Mechanism.* If Vortexa's compliance with Data Protection Legislation applicable to international data transfers is affected by circumstances outside of Vortexa's control, including if a legal instrument for international data transfers is invalidated, amended, or replaced, then Customer and Vortexa will work together in good faith to reasonably resolve such non-compliance. In the event that additional, replacement or alternative transfer mechanisms, standard contractual clauses or UK standard contractual clauses are approved by Supervisory Authorities, Vortexa reserves the right to choose the transfer mechanism of its preference, and amend the Agreement and this DPA by adding to or replacing, the existing transfer mechanism; provided that Vortexa will ensure continued compliance with Data Protection Legislation.

3.9. *Applicability of the Standard Contractual Clauses.* When utilized, the SCCs and the UK Addendum concluded between the parties pursuant to this Section 3 will only apply insofar as strictly necessary for Vortexa to comply with the application Data Protection Legislation.

4. **U.S. Privacy Laws**

4.1. *Applicability.* Section 4 only applies to Vortexa's Processing of Customer Personal Data subject to U.S. Privacy Laws.

4.2. *Compliance Assurance.* If the provision of information provided pursuant to Section 2.12 above does not fulfil the requirements of the applicable U.S. Privacy Laws, Customer has the right to take reasonable and appropriate steps to ensure that Vortexa uses Customer Personal Data consistent with Customer's obligations under applicable U.S. Privacy Laws.

4.3. *Compliance Remediation*. Vortexa shall promptly notify Customer after determining that it can no longer meet its obligations under applicable U.S. Privacy Laws. Upon receiving notice from Vortexa in accordance with this section, Customer may direct Vortexa to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data.

4.4. *Limitations on Processing*. Vortexa will Process Customer Personal Data solely as described in the Agreement and this DPA. Except as expressly permitted therein or by the U.S. Privacy Laws, Vortexa is prohibited from (a) Selling or Sharing Customer Personal Data, (b) retaining, using, or disclosing Customer Personal Data for any other purpose, (c) retaining, using, or disclosing Customer Personal Data outside of the direct business relationship between the parties, and (d) combining Customer Personal Data with Personal Data obtained from, or on behalf of, sources other than Customer or its users, except as expressly permitted under applicable U.S. Privacy Laws.

4.5. *Deletion Requests.* Vortexa shall not be required to delete any Customer Personal Data to comply with a Data Subject's request directed by Customer if retaining such information is specifically permitted by applicable U.S. Privacy Laws; provided, however, that in such case, Vortexa will promptly inform Customer of the exceptions relied upon under applicable U.S. Privacy Laws and Vortexa shall not use Customer Personal Data retained for any purpose other than provided for by that exception.

4.6. *Deidentified Data.* In the event that Customer discloses or makes available deidentified data (as such term is defined in the U.S. Privacy Laws) to Vortexa, Vortexa shall not attempt to reidentify the information.

4.7. *Sale of Data.* The parties acknowledge and agree that the exchange of Personal Data between the parties does not form part of any monetary or other valuable consideration exchanged between the parties with respect to the Agreement or this DPA. Vortexa will never sell Customer's Personal Data.

5. **Security**

5.1. *Vortexa Personnel.* Vortexa will inform its personnel engaged in the Processing of Customer Personal Data of the confidential nature of the Customer Personal Data, and subject them to obligations of confidentiality that survive the termination of that individual's engagement with Vortexa.

5.2. *Third Party Disclosure.* Vortexa will not disclose Customer Personal Data to any third party unless authorized by Customer or required by law. If a government entity (including a law enforcement agency) or Supervisory Authority demands access to Customer Personal Data, Vortexa will attempt to redirect the requestor to request the data directly from Customer or notify Customer prior to disclosure, in each case unless prohibited by law.

5.3. *Security.* Vortexa will implement commercially reasonable technical and organizational measures to safeguard Customer Personal Data taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

6. **Security Breach**

6.1. *Notification Obligations*. Upon becoming aware of any Security Incident affecting Customer Personal Data, the parties shall notify each other without undue delay and shall provide timely updates and information relating to the Security Incident as it becomes known or as is reasonably requested by the other party. Such information will include the nature of the Security Incident, the categories and number of Data Subjects affected, the categories and amount of Customer Personal Data affected, the likely consequences of the Security Incident, and the measures taken or proposed to be taken to address the Security Incident and mitigate possible adverse effects. Vortexa's obligations in this Section 6 do not apply to incidents that are caused by Customer or Customer's personnel or users or to unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

6.2. *Manner of Notification*. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's business, technical or administrative contacts by any means Vortexa selects, including via email. It is Customer's sole responsibility to maintain accurate contact information on Vortexa's systems at all times. Furthermore, it is Customer's sole responsibility to notify the relevant data protection Supervisory Authority and, when applicable, the Data Subjects of a Security Incident as required under the Article 33 and 34 of the GDPR. Vortexa will promptly comply with reasonable requests by Customer to assist it with meeting such notification requirements to the extent Vortexa is legally permitted and able to do so.

7. **Term and Termination**

7.1. *Term of DPA.* This DPA will remain in effect until, and automatically expire upon, deletion of all Customer Personal Data as described in this DPA or when the Customer no longer maintains a subscription to the Service, whichever happens first.

7.2. *Deletion of Customer Personal Data*. Vortexa will delete Customer Personal Data in its possession within 30 days of: (a) receipt of a Customer request that Vortexa delete Customer's account and all associated user accounts; or (b) the date that Customer and all associated users delete their accounts. Prior to deletion, Vortexa will make any Customer Personal Data in its possession available for download by Customer. Vortexa has no obligation to retain any portion of Customer Personal Data after such period except to the extent that Vortexa is required under applicable law to keep a copy of the Customer Personal Data.

8. **Amendment**

8.1 *Amendment.* Vortexa may amend this DPA from time to time. When changes are made, Vortexa will make a new copy of the DPA available at www.vortexa.com/data-processing-agreement/. To the extent an amendment is required to comply with applicable Data Protection Legislation, it will become effective immediately; otherwise, it will be effective upon renewal of Customer's subscription to the Service.

Appendix I - Annex I

A. LIST OF PARTIES

Data Controller/exporter(s):

Customer.

Address: See Agreement and order form.

Contact person's name, position and contact details: Account Owner unless otherwise notified to dpo@vortexa.com

Activities relevant to the data transferred under these Clauses:

Vortexa provides the Service to Customer as described in the Agreement.

Signature and date: Either the date of physical signature on the Agreement or an order form or the date a Customer renews or receives access to the Service.

Vortexa Role (controller/processor): Processor on behalf of Customer, or Subprocessor on behalf of third-party Controller

Data Processor/ importer(s):

Vortexa

B. DESCRIPTION OF TRANSFER

1. *Categories of data subjects whose personal data is transferred*

employees or persons working for Customer in any capacity who Vortexa will coordinate with in respect of the delivery of the Service.

2. *Categories of personal data transferred*

Name, email address and other contact details such as telephone number.

3. *Sensitive data transferred*

N/A.

4. *The frequency of the transfer*

Irregular – at commencement of service and on change of personnel notified to Vortexa

5. *Nature of the Processing*

Collecting, storing, duplicating, deleting, disclosing, and otherwise Processing Customer Personal Data as reasonably necessary in connection with the performance of the Service as described in the Agreement and this DPA.

6. *Purpose(s) of the data transfer and further Processing*

Vortexa will Process Customer Personal Data (i) to perform its obligations pursuant to the Agreement; (ii) to help ensure security and integrity to the extent the use of Customer Personal Data is reasonably necessary and proportionate for these purposes; (iii) to debug, to identify and repair errors that impair existing intended functionality; (iv) to perform other services on behalf of Customer, which may include maintaining or servicing accounts, providing customer support, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing analytics and user outreach; (v) for internal research or analytics for technological development and demonstration; (vi) to undertake activities to verify or maintain the quality or safety of the Service and to improve, upgrade, or enhance the Service; and (vii) as otherwise allowed by the Agreement and this DPA.

7. *The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

For the duration of Customer's subscription to the Service + 30 days

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent Supervisory Authority/ies in accordance with Clause 13: The DPC in Ireland

The competent authority for the processing of Personal Data relating to Data Subjects located in Ireland is the DPC.

Annex II

Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data

This document describes technical and organizational security measures and controls implemented by Vortexa, or Vortexa affiliates (hereafter referred to as Vortexa), to protect personal data and ensure the ongoing confidentiality, integrity, and availability of Vortexa's products and services.

This document is a high-level overview of Vortexa's technical and organizational security measures. More details on the measures we implement are available upon request. Vortexa reserves the right to revise these technical and organizational measures at any time, without notice, so long as any such revisions will not materially reduce or weaken the protection provided for personal data that Vortexa processes in providing its various services. In the unlikely event that Vortexa does materially reduce its security, Vortexa shall notify its customers.

Vortexa shall take the following technical and organizational security measures to protect personal data:

The technical and organisational measures (TOMs) apply to the platforms and services provided by Vortexa with the exception where the Client is responsible for security and privacy TOMs. Evidence of the measures implemented by Vortexa can be provided upon request from the Client.

Policy & Document Management

Vortexa will validate that necessary documentation is in place between Vortexa and the Client where Vortexa processes Personal Data covered by GDPR. Any change to the processing of Client personal data will be reviewed to determine any impact on required TOMs and other existing documentation or contracts. Sub-processors will be identified and available for Client access with periodic review to validate ongoing adherence to the agreed TOMs.

Implementation

- Access to document is limited to nominated individuals within the business
- Request process in place for new sub-processors
- Quarterly meetings scheduled for TOMs review

Security Incidents

Vortexa will maintain an internal incident response plan where the process is documented and followed. The nominated Data Controller will be notified immediately if any known or reasonably suspected breach to Client personal data has been detected.

Implementation

- Incident response plan is hosted within central accessible documentation platform
- Dedicated communication channels are opened with relevant internal stakeholders
- Clients are contact through the existing support channels

Risk Management

Vortexa will assess all risks related, but not limited, to the processing of Client personal data with remediation and mitigation measures of identified risks.

Implementation

- A risk register is hosted and maintained internally
- A risk committee is nominated by the business
- A risk committee reviews existing and new risks quarterly
- Risks are triaged, categorised and prioritised for remediation

Security policies

Vortexa will maintain and follow IT security & cyber security policies that are mandatory for all Vortexa employees to adhere to and acknowledge. IT security and cyber security policies will be reviewed periodically and updated to maintain the protection of the services provided and the processing of Client personal data.

Implementation

- Staff are provided security & compliance training with recorded attendance as part of their onboarding
- Security & compliance training is provided every 12 months from the start date of the member of staff joining
- Security and compliance training is reviewed every 6 months for review and updated based on new threats that have been observed.
- Critical threats are immediately communicated to the business and policies are updated accordingly to respond to these threats

User access management

Vortexa will maintain and review appropriate controls that allow employees access to systems that they truly only need access to. Only employees with clear business justification are provided access to appropriate data, including personal Client data. All additional access requests will be approved on an individual role-based basis and monitored.

All systems and platforms (developed internally or third party) used by Vortexa will adhere to secure minimum authentication requirements stipulated by Vortexa IT. Such as single sign on from our nominated identity provider or enforce multi factor authentication where single sign on is not available.

Implementation

- Staff must comply to the minimum password security set by IT, and they are force enrolled into multi-factor authentication upon sign up on their first day
- Google Workspace is used as the main identity for federated access to our software and platforms

- Platforms that do not support federated authentication have a separate randomly generated password stored within our nominated password manager that is protected by Google Workspace federated authentication

- Staff within Google Workspace are provided access to applications based on the business requirements of them needing access (e.g. commercial cannot access engineering tools)

Endpoint management & protection

Vortexa will provide a company issued device and provide continued maintenance and updates on these devices.

Implementation

- Devices are kept up to date with the latest vendor/manufacturer security updates with a maximum 7-day enforcement period.

- Devices have enforced encryption where the decryption key is stored on a separate database within Azure and only accessible by IT.

- Devices are only usable by the employee that the device is assigned to (no shared devices)

- Firewalls are configured and enforced where employees are unable to permanently change these rules

- Antivirus software is deployed to every employee's device that actively monitors for threats. Threats are immediately quarantined and Vortexa IT are notified for further investigation.

Annex III

The List of Sub-Processors as at the date of this DPA is as follows:

Sub-processor	Nature and Purpose of Processing	Categories of personal data	Location of Processing
Zoom Video Communications, Qumu Corporation	Is used as a webinar platform where emails are processed to send invites to. The users are anonymous to other invitees, this is for internal processing only.	Name (First & Last) Email Address Picture/Video (With consent)	Europe, USA
Google LLC	Google Big Query is used as a data house to store personal data such as their first name, last name and email address. We use this as a central reference point when needing to process this data through other platforms.	Name (First & Last) Email Address	Europe, USA
Slack Technologies	Personal data may be referenced within Slack as part of support interactions and escalations, relating to Vortexa products, between different teams within the business	Name (First & Last) Email Address	USA
Zapier, Inc	Zapier is used to process personal data between company issued registration forms to set up Analyst Webinars.	Name (First & Last) Email Address	USA
Salesforce, Inc	Is used to store personal data and is used as a central reference point to determine access to products based on services they are subscribed to.	Name (First & Last) Email Address	Europe
Gong.io, Inc	Is used to store personal data in the form of videos for pre and post onboarding sessions. These recorded sessions are used to accurately raise feedback. Gong can be used for Google Meet, Zoom and Microsoft Teams but the data is hosted within Gong.	Name (First & Last) Email Address Picture/Video (With consent)	USA
Calendly	These processes nominated personal data to allow clients and prospects to book meetings within times set by owner of the calendar.	Name (First & Last) Email Address	USA
Marketo, Inc.	Stores personal data as a reference point and processed for sending out marketing emails and webinar invitations.	Name (First & Last) Email Address	Europe, USA, Australia
Okta	Auth0 stores personal data that is used as the central authentication for all Vortexa platforms.	Name (First & Last) Email Address	USA
Twillio	SendGrid processes personal data to send email notifications from Vortexa platforms such as password reset requests.	Name (First & Last) Email Address	USA
New Relic, Inc.	May log personal data as we use this platform to stream and store extensive debugging logs from Vortexa's services.	Name (First & Last) Email Address	Europe, USA
Amazon Web Services, Inc.	Stores personal data. All of Vortexa's platform & infrastructure is hosted within Amazon Web Services.	Name (First & Last) Email Address	Europe
Snowflake Computing	We store client Snowflake account information as to use as a reference point to share our services data with them. This account information may have personal data referenced.	Name (First & Last) Email Address	Europe, USA
Microsoft Corporation	Microsoft AppInsights may process personal data, this tool is simply for capturing the telemetry of the Vortexa analytics platform.	Name (First & Last) Email Address	Europe, USA
Fullstory, Inc	Processes personal data against Auth0. This tool records UX actions taken on Vortexa's web platform to help understand behaviour and adapt UX based on common issue patterns.	Name (First & Last) Email Address	USA

An up-to-date list of sub-processors can be found at www.vortexa.com/sub-processors/.