



DOPPEL DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the Doppel Platform Agreement or other software license agreement terms governing the purchase of Doppel's Products (the "**Agreement**") between Doppel Inc. ("**Doppel**") and the customer identified in the Agreement ("**Customer**") (collectively, the "**Parties**"). This Addendum is effective upon your acceptance of the Agreement.

Subject Matter and Duration.

1. **Subject Matter.** This Addendum reflects the Parties' commitment to abide by Applicable Data Protection Laws concerning the Processing of Customer Personal Data in connection with Doppel's execution of the Agreement. All capitalized terms that are not expressly defined in this Data Processing Addendum will have the meanings given to them in the Agreement. If and to the extent language in this Addendum or any of its Exhibits conflicts with the Agreement, this Addendum shall control.
2. **Duration and Survival.** Doppel will Process Customer Personal Data for the term of the Agreement. Doppel's obligations and Customer's rights under this Addendum will continue in effect so long as Doppel Processes Customer Personal Data.
3. **Definitions.** For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.
 - a. "**Administration Data**" means information relating to account administration and billing.
 - b. "**Applicable Data Protection Laws**" means the relevant data protection and data privacy laws, rules and regulations to which the Customer Personal Data are subject. "**Applicable Data Protection Laws**" shall include, but not be limited to, EU General Data Protection Regulation 2016/679 ("**GDPR**") principles and requirements, the United Kingdom Data Protection Act 2018, the Australia Privacy Act 1988, Brazil General Personal Data Protection Law, the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) ("**CCPA**"), and its implementing regulations, and other United States state data protection and privacy laws and regulations similar to or modeled on the CCPA, including the Virginia Consumer Data Protection Act, the Colorado Privacy Act and related regulations, the Utah Consumer Privacy Act, and the Connecticut Act Concerning Personal Data Privacy and Online Monitoring. For the avoidance of doubt, if Doppel's processing activities involving Customer Personal Data are not within the scope of an Applicable Data Protection Law, such law is not applicable for purposes of this Addendum.
 - c. "**Customer Personal Data**" means Personal Data Processed by Doppel on behalf of Customer pursuant to the Agreement. The categories of Customer Personal Data and applicable Processing activities are detailed in Exhibit 1, as required by the GDPR.
 - d. "**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 the Processing of Personal Data.
 - e. "**Controller Purposes**" means the purposes of account administration, billing, and the provision, security, and improvement of the Products and Support.
 - f. "**Deidentified Data**" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable natural person, household, or device, or as otherwise defined under Applicable Data Protection Laws.
 - g. "**Personal Data**" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Laws.
 - h. "**Process**," "**Processes**," "**Processing**," and "**Processed**" mean any operation or set of operations which is performed on data or sets of 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.
 - i. "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Customer Personal Data on behalf of Customer subject to this Addendum.
 - j. "**Security Incident**" means the breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data Processed by Doppel.
 - k. "**Standard Contractual Clauses**" means the UK Standard Contractual Clauses and/or the 2021 Standard Contractual Clauses.
 - l. "**Subprocessor**" means any contractor, agent, vendor or third-party service provider authorized by Doppel to Process Customer Personal Data.
 - m. "**UK Standard Contractual Clauses**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, available at <https://ico.org.uk/media2/migrated/4019539/international-data-transfer-addendum.pdf> and completed as described below.
 - n. "**2021 Standard Contractual Clauses**" means the Standard Contractual Clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses

for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at http://data.europa.eu/eli/dec_impl/2021/914/oj and completed as described below.

- o. **"Usage Data"** means statistical, analytical, and performance data relating to Customer's use of the Products and Support.

Data Use and Processing.

4. **Compliance with Laws.** Customer Personal Data shall be Processed in compliance with the terms of this Addendum and all Applicable Data Protection Laws. Doppel will provide the same level of protection for Customer Personal Data subject to the CCPA as is required of Customer under the CCPA.
5. **Purpose Limitation.** Doppel will not Process Customer Personal Data for any purpose other than for the specific purposes set forth in the Agreement or outside the direct business relationship between Customer and Doppel, unless obligated to do otherwise by applicable law. In such case, Doppel will inform Customer of that legal requirement before the Processing unless legally prohibited from doing so. Doppel shall comply with any applicable restrictions under Applicable Data Protection Laws on combining Customer Personal Data with personal data that Doppel receives from, or on behalf of, another person or persons, or that Doppel collects from any interaction between it and any individual. Notwithstanding the foregoing, Doppel may Process Customer Personal Data for any purposes permitted by Applicable Data Protection Laws for "service providers" (as defined in the CCPA) or Processors to undertake. Further details regarding Doppel's processing operations, including the purposes for processing Customer Personal Data, are set forth in Exhibit 1.
6. **Documented Instructions.** Doppel and its Subprocessors shall Process Customer Personal Data only in accordance with the documented instructions of Customer. The Agreement, including this Addendum, along with any applicable Order, constitutes Customer's complete and final instructions to Doppel regarding the Processing of Customer Personal Data, including for purposes of the Standard Contractual Clauses. Doppel will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions. Doppel acts as an independent Controller with respect to the Processing of Administration Data and Usage Data for the Controller Purposes.
7. **Authorization to Use Subprocessors.** To the extent necessary to fulfill Doppel's contractual obligations under the Agreement or any Order, Customer hereby authorizes (i) Doppel to engage Subprocessors and (ii) Subprocessors to engage subprocessors.
8. **Doppel and Subprocessor Compliance.** Doppel agrees to (i) enter into a written agreement with Subprocessors regarding such Subprocessors' Processing of Customer Personal Data that imposes on such Subprocessors (and their subprocessors) data protection and security requirements for Customer Personal Data that are at least as restrictive as the obligations in this Addendum; and (ii) remain responsible to Customer for Doppel's Subprocessors' (and their subprocessors if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data.
9. **Right to Object to Subprocessors.** Doppel's current list of Subprocessors that Process Customer Personal Data is available in Exhibit 3. Customers may sign up for email notifications of new Subprocessors after logging in to trust.doppel.com. Doppel will provide Customer notice of any new or replacement Subprocessor as soon as reasonably practicable after engagement, including by updating its list of Subprocessors. Customer may object in writing within thirty (30) days after notice on reasonable data-protection grounds. If Customer timely objects on reasonable data-protection grounds, the Parties will work together in good faith to resolve the grounds for the objection for no less than thirty (30) days, and failing any such resolution, Customer may, upon written notice, terminate the part of the Products and Support provided under the Agreement that cannot be performed by Doppel without use of the objectionable Subprocessor.
10. **Confidentiality.** Any person or Subprocessor authorized to Process Customer Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.
11. **Personal Data Inquiries and Requests.** Upon written request from Customer, Doppel agrees to provide reasonable assistance and comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Applicable Data Protection Laws (e.g., access, rectification, erasure, data portability, etc.). If a request is sent directly to Doppel, Doppel shall promptly notify Customer and shall not respond to the request unless Customer has authorized Doppel to do so. Where necessary, Customer shall inform Doppel of any other individual rights requests that Doppel must comply with, and provide the information necessary for Doppel to comply with the request.
12. **Government Access Requests.** Unless prohibited by applicable law or a legally-binding request of law enforcement, Doppel shall promptly notify Customer of any request by government agency or law enforcement authority for access to or seizure of Customer Personal Data, and shall render reasonable assistance to Customer, if Customer wishes to contest the access or seizure.
13. **Data Protection Impact Assessment and Prior Consultation.** Upon written request from Customer, Doppel agrees to provide reasonable assistance at Customer's expense to Customer where, in Customer's judgment, the type of Processing performed by Doppel is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and

systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

14. **Sale or "Sharing" of Customer Personal Data Prohibited.** Doppel shall not sell or share Customer Personal Data as the terms "sell" and "share" are defined by the CCPA.
15. **CCPA Certification.** Doppel hereby certifies that it understands its restrictions and obligations set forth in this Addendum and will comply with them. Doppel will notify Customer if Doppel makes a determination that it can no longer meet its obligations under Applicable Data Protection Laws. Customer shall have the right, upon seven (7) business days' notice, to take reasonable and appropriate steps to stop and remediate any unauthorized use of Customer Personal Data by Doppel.
16. **Deidentified Data.** If Doppel receives Deidentified Data, it will take reasonable measures to ensure it cannot be associated with a data subject, publicly commit to processing it solely in deidentified form without attempting to reidentify it, and contractually obligate recipients to comply with these requirements.

Cross-Border Transfers of Personal Data.

17. **Cross-Border Transfers of Personal Data.** Customer authorizes Doppel and its Subprocessors to transfer Customer Personal Data across international borders, including from the European Economic Area (the "EEA"), the United Kingdom, and Switzerland to the United States. Doppel and Customer agree to use the Standard Contractual Clauses as the transfer mechanism supporting the transfer and Processing of Customer Personal Data, as further detailed below.
18. **2021 Standard Contractual Clauses.** For transfers of Customer Personal Data out of the EEA that are subject to Section 17 of this Addendum, the 2021 Standard Contractual Clauses will apply and are incorporated into this Addendum. For purposes of this Addendum, the 2021 Standard Contractual Clauses will apply as set forth in this Section 18. "Module Two: Transfer controller to processor" will apply and all other module options will not apply. Under Annex 1 of the 2021 Standard Contractual Clauses, the "data exporter" is Customer and the "data importer" is Doppel and the information required by Annex 1 can be found in Exhibit 1. For the purposes of Annex 2 of the Standard Contractual Clauses, the technical and organizational measures implemented by the data importer are those listed in Exhibit 2 of this Addendum. Clause 7 will not apply. For clause 9, the Parties choose Option 2. Section 9 of this Addendum governs Subprocessor objections and remedies. For clause 11, the optional language will not apply. For clause 17, the Parties choose Option 1 and the Parties agree that the governing law will be the Republic of Ireland. For clause 18, the Parties agree that the courts of the Republic of Ireland will apply for subsection (b).
19. **UK Standard Contractual Clauses.** For transfers of Customer Personal Data out of the United Kingdom that are subject to Section 17 of this Addendum, the UK Standard Contractual Clauses will apply and are incorporated into this Addendum. For purposes of this Addendum, the UK Standard Contractual Clauses will apply as set forth in this Section 19. For Table 1 of the UK Standard Contractual Clauses, (i) the Parties' details shall be the Parties and their Affiliates to the extent any of them is involved in such transfer, including those set forth in Annex 1 of the 2021 Standard Contractual Clauses and (ii) the Key Contacts shall be the contacts set forth in Annex 1 of the 2021 Standard Contractual Clauses. The Approved EU SCCs referenced in Table 2 shall be the 2021 Standard Contractual Clauses as executed by the Parties pursuant to this Addendum. For Table 3, the information for Annexes I.A and I.B is set forth in Exhibit 1, the information for Annex II is set forth in Exhibit 2, and the list of Subprocessors is set forth in Exhibit 3 of this Addendum. For Table 4, either party may end the UK Standard Contractual Clauses as set out in Section 19 of the UK Standard Contractual Clauses.
20. **Switzerland Transfers.** For transfers of Customer Personal Data out of Switzerland that are subject to Section 17 of this Addendum, the 2021 Standard Contractual Clauses will apply and will be deemed to have the differences set forth in this Section 20, to the extent required by the Swiss Federal Act on Data Protection ("FADP"). References to the GDPR in the 2021 Standard Contractual Clauses are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR. The term "member state" in the 2021 Standard Contractual Clauses shall not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the 2021 Standard Contractual Clauses. Under Annex I(C) of the 2021 Standard Contractual Clauses (Competent supervisory authority): where the transfer is subject exclusively to the FADP and not the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner, and where the transfer is subject to both the FADP and the GDPR, the supervisory authority is the Swiss Federal Data Protection and Information Commissioner insofar as the transfer is governed by the FADP, and the supervisory authority is as set forth in the 2021 Standard Contractual Clauses insofar as the transfer is governed by the GDPR.
21. Each party's signature to this Addendum shall be considered a signature to the Standard Contractual Clauses. If required by the laws or regulatory procedures of any jurisdiction, the Parties shall execute or re-execute the Standard Contractual Clauses as separate documents. In case of conflict between the Standard Contractual Clauses and this Addendum, the Standard Contractual Clauses will prevail.

Information Security Program.

22. **Information Security Program.** Doppel agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as required by Applicable Data Protection Laws. Such measures

shall be designed to include those measures set forth in **Exhibit 2 - Technical and Organizational Security Measures**.

Security Incident Procedure.

23. Doppel will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to reasonably suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.
24. **Notice.** Doppel agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Laws (but in no event longer than forty-eight (48) hours) to Customer's Designated POC upon becoming aware that a Security Incident has taken place. Such notice will include all available details required under Applicable Data Protection Laws for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

Audits.

25. **Right to Audit; Permitted Audits.** Doppel shall make available to Customer and its regulators all information necessary to demonstrate compliance with Applicable Data Protection Laws and this Addendum. Customer and its regulators shall have the right to inspect Doppel's architecture, systems, and documentation which are relevant to the security and integrity of Customer Personal Data, or as otherwise required by a governmental regulator:
 - a. Following any notice from Doppel to Customer of an actual Security Incident involving Customer Personal Data;
 - b. Upon Customer's reasonable belief that Doppel is not in compliance with Applicable Data Protection Laws, this Addendum or its security policies and procedures under the Agreement;
 - c. As required by governmental regulators;
26. **Audit Terms.** Any audits described in this Section shall be:
 - a. Conducted by Customer or its regulator, or through a third party independent contractor selected by one of these parties, and to whom Doppel does not reasonably object.
 - b. Conducted during reasonable times.
 - c. Conducted upon reasonable advance notice to Doppel.
 - d. Of reasonable duration and scope and shall not unreasonably interfere with Doppel's day-to-day operations.
 - e. Conducted in such a manner that does not violate any agreement between Doppel and its service providers, including cloud providers, or violate or cause Doppel to violate its reasonable policies related to security and confidentiality.
27. **Third Parties.** In the event that Customer conducts an audit through a third party independent auditor or a third party accompanies Customer or participates in such audit, such third party shall be required to enter into a non-disclosure agreement containing confidentiality provisions substantially similar to those set forth in the Agreement to protect Doppel's and Doppel's customers' confidential and proprietary information. For the avoidance of doubt, regulators shall not be required to enter into a non-disclosure agreement.
28. **Audit Results.** Upon Doppel's request, after conducting an audit, Customer shall notify Doppel of the manner in which Doppel does not comply with any of the applicable security, confidentiality or privacy obligations or Applicable Data Protection Laws herein. Upon such notice, Doppel shall make any necessary changes to ensure compliance with such obligations at its own expense and without unreasonable delay and shall notify Customer when such changes are complete. Notwithstanding anything to the contrary in the Agreement, Customer may conduct a follow-up audit within six (6) months of Doppel's notice of completion of any necessary changes. To the extent that a Customer audit identifies any material security vulnerabilities, Doppel shall promptly remediate those vulnerabilities.

Data Storage and Deletion.

29. **Data Storage.** Doppel will not store or retain any Customer Personal Data except as necessary to provide the Products and Support under the Agreement.
30. **Data Deletion.** Doppel will abide by the following with respect to deletion of Customer Personal Data:
 - a. Within sixty (60) calendar days of the Agreement's expiration or termination, Doppel will securely destroy (per Section 30(c) below) all copies of Customer Personal Data (including automatically created archival copies).
 - b. Upon Customer's request, Doppel will promptly return to Customer a copy of all Customer Personal Data within thirty (30) calendar days and, if Customer also requests deletion of the Customer Personal Data, will carry that out as set forth above.
 - c. All deletion of Customer Personal Data will be conducted in accordance with standard industry practices for deletion of sensitive data.
 - d. Tapes, printed output, optical disks, and other physical media will be physically destroyed by a secure method, such as shredding performed by a bonded provider.
 - e. Upon Customer's request, Doppel will provide evidence that Doppel has deleted all Customer Personal Data. Doppel will provide the "Certificate of Deletion" within thirty (30) calendar days of Customer's

request.

Contact Information.

31. Doppel and the Customer agree to designate a point of contact for urgent privacy and security issues (a “**Designated POC**”). The Designated POCs for the Parties are:

Doppel Designated POC:	Legal Department; privacy@doppel.com
Customer Designated POC:	The individual and/or email specified in the Notices section of the Agreement, or if not specified, the individual or email specified herein. Name: Title: Email: Phone (if applicable):

Exhibit 1

Doppel Processing Details

Processing details for the Doppel Products and Support, forming part of the data processing terms agreed with our customers.

Capitalized terms used herein shall have the meanings ascribed to them in the data processing terms entered into between Doppel and its customers. Doppel may change these processing details from time to time and where required will notify customers of material changes.

Products Covered.

PRODUCT	SCOPE
Digital Risk Protection	Monitoring for misuse of Customer's brand and employee identities and facilitating related takedown activity.
Email Security	Email threat detection, classification and remediation, including anti-spam, anti-virus, URL and attachment analysis and sandboxing.
Human Risk Management	Security awareness training, phishing simulations, end-user nudges and related reporting and scorecards.

Processing Details.

LIST OF PARTIES

Data Exporter — Customer

Name: The relevant customer entity, as identified in the applicable Order, who, acting as Controller, transfers the Personal Data to Doppel

Address: Addresses are specified in the applicable Order

Contact: Customer contact details are specified in the applicable Order

Activities: See Nature and Purpose of Processing below

Role: Controller

Data Importer — Doppel

Name: Doppel, as identified in the applicable Order, who, acting as Processor, agrees to receive Personal Data from the Data Exporter

Address: Addresses are identified in the applicable Order

Contact: Legal Department, privacy@doppel.com

Activities: See Nature and Purpose of Processing below

Role: Processor

COMPETENT SUPERVISORY AUTHORITY (ANNEX I.C)

The Irish Data Protection Commission will be the competent supervisory authority where permitted by Clause 13. Otherwise, the authority will be the authority responsible for Customer's compliance regarding the transfer, or, where Customer is not established in the EEA, the authority for its GDPR representative's location. If Customer is exempt from appointing a representative, Customer will identify before transfer an authority where affected data subjects are located, as required by Clause 13.

CATEGORIES OF DATA SUBJECTS

Personal Data Processed in the provision of Products and Support may include data related to the following categories of data subjects:

- Customer's employees, agents, consultants, freelancers and contractors;
- Users and other participants from time to time to whom the Customer has granted the right to access the Products in accordance with the Agreement;
- Customer's service providers; and/or other individuals to the extent identifiable in the content of emails, other messaging services, their attachments, or in archiving content.

CATEGORIES OF PERSONAL DATA

The Personal Data Processed concerns the following categories:

- Personal details (e.g., names, user names, passwords, email addresses and/or IP addresses, current and past home address, phone number);
- Personal Data derived from the use of the Products such as login records, alerts and general analytics;
- Personal Data within email and/or messaging content which identifies, or may reasonably be used to identify, data subjects;
- Personal Data included within metadata including, but not limited to, the following fields: sent, to, from, date, time, subject, URL, email address, and/or IP address;
- Personal Data provided to Doppel via the Product, by (or at the direction of) Customer or by its Users.

SPECIAL CATEGORIES OF DATA

No sensitive data or special categories of data are intended to be Processed but may be contained in the content of or attachments to email and/or other messages. The extent of Personal Data Processed is determined and controlled by the Customer.

FREQUENCY OF PROCESSING

Continuous and ongoing during the term of the Agreement.

NATURE AND PURPOSE OF THE PROCESSING

- **Provision of Products and Support.** Personal Data will be Processed in accordance with Customer's instructions.
- **Support.** Technical support, issue diagnosis and error correction to ensure the efficient and proper running of the systems for the provision of the Products and specifically in answer to a customer query. This operation relates to Personal Data Processed through the Product. Such will be limited to metadata where possible.
- **Usage Data.** Doppel also Processes certain data derived from the Products, including utilization statistics, reports, configuration data, logs, and information regarding spam, viruses and/or other malware. Doppel owns all aggregated Usage Data.

DURATION OF THE PROCESSING

The Customer Personal Data Processed by Doppel will be Processed for the duration of the Agreement.

Product-Specific Processing.

The table below identifies additional processing details for the noted Products.

PRODUCT	EXCEPTION DETAILS
Digital Risk Protection	<i>Categories of data subjects</i>
	Personal Data derived from monitoring via DRP Products (name, physical addresses, telephone numbers, email addresses, IP addresses); Personal Data within email and/or messaging content which identifies or may reasonably be used to identify data subjects if a takedown is requested.
Email Security	<i>Nature and Purpose of Processing</i>
	URL Scanning. URL scanning for the purposes of the provision of threat protection and similar services. This operation relates to attachments and links in emails and/or messaging and will relate to any Personal Data within those attachments or links, which could include all categories of Personal Data.
Human Management	Risk <i>Categories of data subjects</i>
	Customer's employees, consultants, contractors and/or agents whose information is provided to Doppel or who access or use the HRM Products under the Agreement.
	<i>Categories of Personal Data</i> Business identity and contact information, including name, work email address, and optional work phone number, which may include a personal mobile number where used for work purposes; and employment attributes, including department, title or employee level, manager, country or work location, language, timezone, start date, and employment status. Employment attributes are optional and depend on the

information Customer chooses to provide or synchronize with Doppel.

Voice and Facial Data

Voice or facial data provided by the Customer is Processed as Personal Data and is not used for biometric identification or to uniquely identify an individual.

Nature and Purpose of Processing

Providing Customer's Users with access to the HRM Products; administering and supporting Customer's use of the HRM Products; providing cybersecurity awareness training and authorized security simulations; maintaining, securing, and optimizing the HRM Products; and complying with applicable legal or regulatory obligations.

Exhibit 2

Technical and Organizational Security Measures

Introduction

Doppel employs a combination of policies, procedures, guidelines and technical and physical controls to protect the personal data it processes from accidental loss and unauthorized access, disclosure or destruction.

Governance and Policies

Doppel assigns personnel with responsibility for the determination, review and implementation of data handling policies and measures.

Doppel:

- has a documented data handling policy and/or other relevant guidelines and documents; and
- reviews its security measures and policies to ensure they continue to be appropriate for the data being protected.

Doppel establishes and follows secure configurations for systems and software, and ensures that security measures are considered during project initiation and the development of new IT systems.

Breach response

Doppel has an incident response plan that has been developed to address data breach events.

Intrusion, anti-virus and anti-malware defences

Doppel's IT systems used to process personal data have appropriate data security software installed on them, including:

- firewall, anti-virus system and anti-spyware system;
- an intrusion detection or prevention system managed outside of the control of system and network administrators;
- third-party penetration testing;
- vulnerability scanning;
- collection, maintenance, review and audit of event logs; and
- monitoring of Doppel's cloud service operation.

Access controls

Doppel limits access to personal data by implementing appropriate access controls, including:

- limiting administrative access privileges and use of administrative accounts;
- access to data received from the Customer is granted only for justifiable business cases, such as debugging failures, machine learning training problems or other operational issues;
- employee access to production is guarded by an approval process. When access is approved, access is granted on a temporary basis;
- monitoring and logging access to IT systems; and
- monitoring and logging amendments to data or files on IT systems.

Availability and Back-up personal data

Doppel has a documented disaster recovery plan that ensures that key systems and data can be restored in the event of a physical or technical incident.

Doppel regularly backs up information on IT systems and keeps back-ups in separate locations.

Segmentation of personal data

Doppel logically separates Customer Personal Data at the database/datastore level using a unique identifier for Customer. The separation is enforced at the API layer where Customer must authenticate with a chosen account and then the customer unique identifier is included in the access token and used by the API to restrict access to data to the account. All database/datastore queries then include the account identifier.

Encryption

All databases, data stores and file systems are encrypted according to Doppel's Encryption Policy.

Data at rest is encrypted using industry standard 256-bit Advanced Encryption Standard.

Doppel supports the latest recommended secure cipher suites to encrypt all traffic in transit, including the use of TLS 1.2 protocols, AES256 encryption and SHA2 signatures.

Transmission or transport of personal data

Appropriate controls are implemented by Doppel to secure personal data during transmission or transit, including:

- use of VPNs;
- encryption in transit; and
- logging of access when transmitted electronically.

Device hardening

Doppel ensures that all virtual machines are hardened in accordance with the Center for Internet Security Benchmarks.

Asset and Software management

Doppel maintains an inventory of IT assets and the data stored on them, together with a list of owners of the relevant IT assets.

Doppel:

- documents and implements rules for acceptable use of IT assets;
- requires network level authentication and uses client certificates to validate and authenticate systems;
- deploys automated patch management tools and software update tools for operating systems and software;
- proactively monitors software vulnerabilities and promptly implements any out of cycle patches; and
- permits the use of only the latest versions of fully supported web browsers and email clients.

Doppel stores all API keys securely, including as follows:

- Doppel stores API keys directly in its environment variables;
- Doppel does not store API keys on client side;
- Doppel does not publish API key credentials in online code repositories (whether private or not); and
- Doppel uses API key management tools to retrieve and manage credentials for large development projects.

Physical security

Doppel implements physical security measures to safeguard personal data. This may include:

- Deployment of appropriate building security, including visitor logs, ID card access for staff and contractors, logs of staff access to buildings, and video security.
- Deployment and enforcement of appropriate policies to ensure that:
 - Personal data is printed only where this is necessary for a person to perform his/her job role.
 - Sensitive personal data or large amounts of personal data held in hardcopy are kept in a secure location. Generally, steps are taken to ensure that access to hardcopy personal data is limited in the same way it would be on an electronic IT system i.e., access is limited to those individuals where it is necessary for them to have access to perform their job role.
 - Hardcopy documents containing personal data are only taken off site where necessary for a person's job role.
 - When travelling or working away from the office hard copy documents and portable devices containing personal data are kept secure e.g., never left in a car or unsecured in a public place.
 - Paper records which contain confidential information (including personal data and Sensitive personal data) are shredded after use.

Staff training and awareness

Doppel's agreements with staff and contractors and employee handbooks set out its personnel's responsibilities in relation to information security.

Doppel carries out:

- regular staff training on data security and privacy issues relevant to their job role and ensures that new starters receive appropriate training before they start their role (as part of the onboarding procedures);
- appropriate screening and background checks on individuals that have access to sensitive personal data.

Doppel ensures that information security responsibilities that are applicable immediately before termination or change of employment and those which apply after termination / change of employment are communicated and implemented.

Staff are subject to disciplinary measures for breaches of Doppel's policies and procedures relating to data privacy and security.

Selection of service providers and commission of services

Doppel assesses service providers' ability to meet their security requirements before engaging them.

Doppel has written contracts in place with service providers which require them to implement appropriate security measures to protect the personal data they have access to and limit the use of personal data in accordance with Doppel's instructions.

The Data Importer conducts audits of vendors (including Subprocessors) that have access to Doppel's data by reviewing vendors' security accreditation (such as ISO 27001 or SOC 2) reports.

Exhibit 3**Subprocessors**

Subprocessor	Service Provided	Location
Auth0	Authentication service	USA
DocuSign	E-signature Platform	USA
Google Cloud Platform	Cloud service provider	USA
Google Workspace	Email, file storage	USA
Hasura	API layer	USA
Microsoft Teams	Customer communications	USA
Optery	PII removal	USA
Pylon	Customer engagement tracking	USA
Salesforce	Customer relationship management	USA
Slack	Customer communications	USA
Zoom	Video conferencing provider	USA
ZoomInfo	Contact and business information gathering	USA
Reachdesk	Direct mail, corporate gifting, and fulfillment platform supporting customer engagement, events, and relationship-building activities	USA
Merge	API integration platform used to connect, sync, and manage data between Doppel and authorized third-party business systems	USA
Skyflow	Integrations and agent-tools provider used to protect sensitive data through encryption and tokenization	USA
Claude	AI language model platform	USA
Crayon	Competitive intelligence platform	USA
HeyGen	AI-powered video generation, including video, transcript, and translation services	USA
OpenAI	AI language model / natural language processing platform	USA
ChurnZero	Customer success platform for account/usage analytics, customer journeys, reporting, alerts, and renewal management	USA