**Data Processing Agreement**

Updated April 8, 2024

# Overview

This Data Processing Agreement ("DPA") includes Standard Contractual Clauses adopted by the European Commission, as applicable, and defines our ("Exit Path", "we", "our", or "us") agreement with you ("your", "you", "Customer", "your business", "user", including "your users") with respect to the Processing of Personal Data under the Exit Path Terms of Service ("TOS") and with the most up-to-date version of the TOS located at [www.exitpath.ai/terms](www.exitpath.ai/terms). The TOS and DPA collectively form the Exit Path agreement with you (the "Agreement").

# 1. Definitions

**"California Personal Information"** means Personal Data that is subject to the protection of the CCPA. "CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

**"Consumer", "Business", "Sell" and "Service Provider"** will have the meanings given to them in the CCPA.

**"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.

**"Data Protection Laws"** means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated or replaced from time to time.

**"Data Subject"** means the individual to whom Personal Data relates or belongs.

**"Europe"** means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

**"European Data"** means Personal Data that is subject to the protection of European Data Protection Laws.

**"European Data Protection Laws"** means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) in respect of the United Kingdom, any applicable national legislation that replaces or converts in domestic law the GDPR or any other law relating to data and privacy as a consequence of the United Kingdom leaving the European Union; and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance; in each case, as may be amended, superseded or replaced.

**"Instructions"** means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

**"Permitted Affiliates"** means any of your Affiliates that (i) are permitted to use our Services pursuant to the Agreement, but have not signed their own separate agreement, (ii) qualify as a Controller of Personal Data

Processed by us, and (iii) are subject to European Data Protection Laws.

**"Personal Data"** means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

**"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

**"Privacy Shield"** means the EU-U.S. and Swiss-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to its Decision of July, 12 2016 and by the Swiss Federal Council on January 11, 2017 respectively; as may be amended, superseded or replaced. "Privacy Shield Principles" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Exhibit II to the European Commission Decision of July, 12 2016; as may be amended, superseded or replaced.

**"Processing"** means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly.

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

**"Standard Contractual Clauses"** means the standard contractual clauses for Processors approved pursuant to the European Commission's decision (C(2010)593) of 5 February 2010, in the form set out at Exhibit 3; as may be amended, superseded or replaced.

**"Sub-Processor"** means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Services under the Agreement. Sub-Processors may include third parties or our Affiliates but excludes any Exit Path employee or consultant.

# 2. Customer Responsibilities

a. Compliance with Laws. Within the scope of the Agreement and in its use of the Services, you will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to us.

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which you acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Services, including those relating to obtaining consents (where required) to send emails, the content of the emails and its email deployment practices. You will inform us without undue delay if it is not able to comply with its responsibilities under this sub-section (a) or applicable Data Protection Laws.

b. <u>Controller Instructions.</u> The parties agree that the Agreement (including this DPA), together with your use of the Service in accordance with the Agreement, constitute your complete and final Instructions to us in relation to the Processing of Personal Data, and additional instructions outside the scope of the Instructions shall require prior written agreement between us and you.

## 3. Exit Path Obligations

a. <u>Compliance with Instructions.</u> We will only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

b. <u>Conflict of Laws.</u> If we become aware that we cannot Process Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable Services until such time as you issue new lawful Instructions with regard to the Processing.

c. <u>Security.</u> We will implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Exhibit 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

d. <u>Confidentiality.</u> We will ensure that any personnel whom we authorize to Process Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e. <u>Personal Data Breaches.</u> We will notify you without undue delay after it becomes aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

f. <u>Deletion or Return of Personal Data.</u> We will delete or return all Customer Data, including Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of your Service in accordance with the procedures and timeframes set out in the Agreement, save that this requirement shall not apply to the extent we are required by applicable law to retain some or all of the Customer Data, or to Customer Data it has archived on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with its deletion practices. You may request the deletion of your Exit Path account after expiration or termination of Service by sending a request to [support@exitpath.ai](mailto:support@exitpath.ai)

## 4. Data Subject Requests

The Service provides limited controls to retrieve, correct, delete or restrict Personal Data from your end users, as most of this data is managed by Processors and Sub-Processors which collect and make this data accessible to the Service. You can limit our access to this data by removing your connection to the Service. To the extent that you are unable to independently address a Data Subject Request directly through our Service, then upon your written request we will provide reasonable assistance in the removal of such Personal Data from other Processors and Sub-Processors and you shall reimburse us for the commercially reasonable costs arising from this assistance.

# 5. Sub-Processors

You agree that we may engage Sub-Processors to Process Personal Data on your behalf. We have currently appointed, as Sub-Processors, Exit Path Affiliates and third parties listed in Exhibit 4 to this DPA. We will notify you if we add or remove Sub-Processors to Exhibit 4 prior to any such changes, primarily through an update to this agreement. Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will make commercially reasonable efforts to ensure each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.

# 6. Data Transfers

You acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Service in accordance with the Agreement, and in particular that Personal Data will be transferred to and processed by Exit Path, Inc. in the United States and to other jurisdictions where Exit Path Processors, Sub-Processors and Affiliates maintain operations. We will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

# 7. Additional Provisions for European Data

a. <u>Scope of Section 7.</u> This 'Additional Provisions for European Data' section shall apply only with respect to European Data.

b. <u>Roles of the Parties.</u> When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of European Data and we are the Processor.

c. <u>Instructions.</u> If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay.

d. <u>Notification and Objection to New Sub-Processors.</u> We will notify you of any changes to Sub-processors by updating Exhibit 4 to this DPA and will give you the opportunity to object to the engagement of the new Sub-Processor on reasonable grounds relating to the protection of Personal Data within 30 days after updating Exhibit 4 to this DPA. If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the Service in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination or Service).

e. <u>Data Protection Impact Assessments and Consultation with Supervisory Authorities.</u> To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities or other competent data privacy authorities to the extent required by European Data Protection Laws.

f. <u>Transfer Mechanisms for Data Transfers.</u>

(A) Exit Path shall not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism

recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

(B) You acknowledge that in connection with the performance of the Services, Exit Path, Inc. is a recipient of European Data in the United States and Canada. The parties acknowledge and agree to the following:

(a) Standard Contractual Clauses: Exit Path, Inc. agrees to abide by and process European Data in compliance with the Standard Contractual Clauses.

(b) Privacy Shield: Although Exit Path, Inc. does not rely on the EU-US Privacy Shield as a legal basis for transfers of Personal Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for as long as Exit Path, Inc. is self-certified to the Privacy Shield Exit Path Inc. will process European Data in compliance with the Privacy Shield Principles and let you know if it is unable to comply with this requirement.

(C) The parties agree that (i) purely for the purposes of the descriptions in the Standard Contractual Clauses, Exit Path Inc. will be deemed the "data importer" and Customer will be deemed the "data exporter" (notwithstanding that you may yourself be located outside Europe and/or be acting as a processor on behalf of third party controllers), (ii) notwithstanding the foregoing, where the Exit Path contracting entity under the Agreement is not Exit Path, Inc., You provide such contracting entity with a mandate to enter into the Standard Contractual Clauses with Exit Path, Inc. in its name and on its behalf, such contracting entity (not Exit Path, Inc.) will remain fully and solely responsible and liable to you for the performance of the Standard Contractual Clauses by Exit Path, Inc., and you will direct any instructions, claims or enquiries in relation to the Standard Contractual Clauses to such contracting entity; and (iii) if and to the extent the Standard Contractual Clauses (where applicable) conflict with any provision of this DPA, the Standard Contractual Clauses will prevail to the extent of such conflict.

g. Demonstration of Compliance.We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections by you in order to assess compliance with this DPA. You acknowledge and agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this sub-section (g). You acknowledge that the Service is hosted by our data center partners who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are regularly tested by independent third party penetration testing firms. Upon request, we will supply (on a confidential basis) a summary copy of its penetration testing report(s) to you so that you can verify our compliance with this DPA. Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year.

## 8. Additional Provisions for California Personal Information

a. Scope of Section 8. The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

b. Roles of the Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA.

c. Responsibilities. The parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services and Consulting Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA, including as described in the 'Data Practices and Machine Learning' section of our Product Specific Terms.

# 9. General Provisions

a. <u>Amendments.</u> Notwithstanding anything else to the contrary in the Agreement and without prejudice to the 'Compliance with Instructions' or 'Security' sections of this DPA, we reserve the right to make any updates and changes to this DPA and the terms that apply in the 'Amendment; No Waiver' section of the Master Terms will apply.

b. <u>Severability.</u> If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

c. <u>Limitation of Liability.</u> Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' section of the Master Terms and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA). For the avoidance of doubt, if Exit Path Inc. is not a party to the Agreement, the 'Limitation of Liability' section of the Master Terms will apply as between you and Exit Path Inc., and in such respect any references to Exit Path, 'we', 'us' or 'our' will include both Exit Path Inc. and the Exit Path entity that is a party to the Agreement.

d. <u>Governing Law.</u> This DPA will be governed by and construed in accordance with the 'Contacting Entity; 'Applicable Law; Notice' sections of the Jurisdiction Specific Terms, unless required otherwise by Data Protection Laws.

# 10. Parties to this DPA

a. <u>Permitted Affiliates.</u> By signing the Agreement, you enter into this DPA on behalf of yourself and, to the extent required under applicable Data Protection Laws, in the name and on behalf of your Permitted Affiliates, thereby establishing a separate DPA between us and each such Permitted Affiliate subject to the Agreement and the 'General Provisions' and 'Parties to this DPA' sections of this DPA. Each Permitted Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the purposes of this DPA only, and except where indicated otherwise, the terms "Customer", "you" and "your" will include you and such Permitted Affiliates.

b. <u>Authorization.</u> The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. <u>Remedies.</u> Except where applicable Data Protection Laws require a Permitted Affiliate to exercise a right or seek any remedy under this DPA against us directly by itself, the parties agree that (i) solely the Customer entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all communication with us under the DPA and will be entitled to make and receive any communication related to this DPA on behalf of its Permitted Affiliates.

d. <u>Other rights.</u> The parties agree that you will, when reviewing our compliance with this DPA pursuant to the 'Demonstration of Compliance' section, take all reasonable measures to limit any impact on us and our Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Permitted Affiliates in one single audit.

# Exhibit 1 - Details of Processing

This Exhibit forms part of the DPA.

A. Nature and Purpose of Processing
We will Process Personal Data as necessary to provide the Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by you in your use of the Services.

B. Duration of Processing
Subject to the 'Deletion or Return of Personal Data' section of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

C. Categories of Data subjects
You may submit Personal Data in the course of using the Service, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects: Your Contacts and other end users including your employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects may also include individuals attempting to communicate with or transfer Personal Data to your end users.

D. Categories of Personal Data
You may submit Personal Data to the Services, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

- Contact Information (as defined in the Master Terms).
- Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Service.

E. Special categories of data (if appropriate)
The parties do not anticipate the transfer of special categories of data.

F. Processing operations Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

a. Storage and other Processing necessary to provide, maintain and improve the Services provided to you; and/or

b. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

# Exhibit 2 - Security Measures

This Exhibit forms part of the DPA.

We currently observe the Security Measures described in this Exhibit 2. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Master Terms.

a) Access Control

i) Preventing Unauthorized Product Access
Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options.

Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use
We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

Static code analysis: Security reviews of code stored in our source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

Bug bounty: A bug bounty program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. We implement a bug bounty program in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

iii) Limitations of Privilege & Authorization Requirements
Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Employee roles are reviewed at least once every six months.

Background checks: All Exit Path employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All Exit Path employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control
In-transit: We make HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the Exit Path products. Our HTTPS implementation uses industry standard algorithms and certificates. At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents. Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

d) Availability Control Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

# Exhibit 3 - Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, The Customer, as defined in the Exit Path Customer Terms of Service (the "data exporter")

And

Exit Path Inc., 3917 Donna Dr., Huntingdon Valley, Pennsylvania 19006 (the "data importer")

each a 'party'; together 'the parties', HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

**Clause 1**

**Definitions**

For the purposes of the Clauses:

'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

'the data exporter' means the controller who transfers the personal data; 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer

in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**Clause 2**

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

**Clause 3**

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

**Clause 4**

Obligations of the data exporter

The data exporter agrees and warrants: (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data

protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

**Clause 5**

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

**Clause 6**

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data

importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

**Clause 7**

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

**Clause 8**

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

**Clause 9**

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

**Clause 10**

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

**Clause 11**

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are

imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

**Clause 12**

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the subprocessor shall, at the choice of the data exporter, destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

# Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

Defined terms used in this Appendix 1 shall have the meaning given to them in the Agreement (including the DPA).

**Data exporter**

The data exporter is the legal entity specified as "Customer" in the DPA.

**Data importer**

The data importer is Exit Path Inc.

**Data subjects**

Please see Exhibit 1 of the DPA, which describes the data subjects.

**Categories of data**

Please see Exhibit 1 of the DPA, which describes the categories of data.

**Special categories of data (if appropriate)**

The parties do not anticipate the transfer of special categories of data.

**Purposes of Processing**

Exit Path Inc. shall process personal data as necessary to provide the Services to data exporter in accordance with the Agreement.

**Processing operations**

Please see Exhibit 1 of the DPA, which describes the processing operations.

# Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses'). Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see Exhibit 2 of the DPA, which describes the technical and organisational security measures implemented by Exit Path.

# Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

This Appendix sets out the parties' interpretation of their respective obligations under specific terms of the Clauses. Where a party complies with the interpretations set out in this Appendix, that party shall be deemed by the other party to have complied with its commitments under the Clauses.

For the purposes of this Appendix, "DPA" means the Data Processing Agreement in place between Customer and Exit Path and to which these Clauses are incorporated and "Agreement" shall have the meaning given to it in the DPA. Clause 4(h) and 8: Disclosure of these Clauses

a. Data exporter agrees that these Clauses constitute data importer's Confidential Information as that term is defined in the Agreement and may not be disclosed by data exporter to any third party without data importer's prior written consent unless permitted pursuant to Agreement. This shall not prevent disclosure of these Clauses to a data subject pursuant to Clause 4(h) or a supervisory authority pursuant to Clause 8.

Clauses 5(a) and 5(b): Suspension of data transfers and termination

a. The parties acknowledge that data importer may process the personal data only on behalf of the data exporter and in compliance with its instructions as provided by the data exporter and the Clauses.

b. The parties acknowledge that if data importer cannot provide such compliance in accordance with Clause 5(a) and Clause 5(b) for whatever reason, the data importer agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract the affected parts of the Services in accordance with the terms of the Agreement.

c. If the data exporter intends to suspend the transfer of personal data and/or terminate the affected parts of the Services, it shall endeavour to provide notice to the data importer and provide data importer with a reasonable period of time to cure the non-compliance ("Cure Period").

d. If required, the parties shall reasonably cooperate with each other during the Cure Period to agree what additional safeguards or other measures, if any, may be reasonably required to ensure the data importer's compliance with the Clauses and applicable data protection law.

e. If after the Cure Period the data importer has not or cannot cure the non-compliance then the data exporter may suspend and/or terminate the affected part of the Services in accordance with the provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by the data exporter prior to suspension or termination). The data exporter shall not be required to provide such notice in instance where it considers there is a material risk of harm to data subjects or their personal data.

Clause 5(f): Audit

a. Data exporter acknowledges and agrees that it exercises its audit right under Clause 5(f) by instructing data importer to comply with the audit measures described in the 'Demonstration of Compliance' section of the DPA.

Clause 5(j): Disclosure of subprocessor agreements

a. The parties acknowledge the obligation of the data importer to send promptly a copy of any onward subprocessor agreement it concludes under the Clauses to the data exporter.

b. The parties further acknowledge that, pursuant to subprocessor confidentiality restrictions, data importer may be restricted from disclosing onward subprocessor agreements to data exporter. Notwithstanding this, data importer shall use reasonable efforts to require any subprocessor it appoints to permit it to disclose the subprocessor agreement to data exporter.

c. Even where data importer cannot disclose a subprocessor agreement to data exporter, the parties agree that, upon the request of data exporter, data importer shall (on a confidential basis) provide all information it reasonably requires in connection with such subprocessing agreement to data exporter.

Clause 6: Liability

a. Any claims brought under the Clauses shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement. In no event shall any party limit its liability with respect to any data subject rights under these Clauses.

Clause 11: Onward subprocessing

a. The parties acknowledge that, pursuant to FAQ II.1 in Article 29 Working Party Paper WP 176 entitled "FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC" the data exporter may provide a general consent to onward subprocessing by the data importer.

b. Accordingly, data exporter provides a general consent to data importer, pursuant to Clause 11 of these Clauses, to engage onward subprocessors. Such consent is conditional on data importer's compliance with the requirements set out in the 'Notification and Objection to New Sub-Processors' section of the DPA.

Clause 12: Obligation after the termination of personal data-processing services

a. Data importer agrees that the data exporter will fulfil its obligation to return or destroy all the personal data on the termination of the provision of data-processing services by complying with the 'Deletion or Return of Personal Data' section of the DPA.

# Exhibit 4 - List of Sub-Processors

| Data Service | Purpose | Location |
|---|---|---|
| Amazon Web Services, Inc. | Data processing and storage, Email sending | United States |
| Google, LLC. | User Authentication, Data processing, Data Storage | United States |
| OpenAI | Natural Language Processing, Conversational AI, Data processing | United States |
| Facebook | User Authentication, Data processing | United States |
| Cloudflare, Inc. | Content Delivery Network | United States |
| Stripe | Data storage and payment processing | United States |

## More Information

If you have any questions regarding this DPA or the Services we provide, please contact us at [support@exitpath.ai](mailto:support@exitpath.ai).