

OPENPROVIDER - DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "DPA") is executed by and between you ("Client") and the Openprovider (trade name of Hosting Concepts B.V., established in Rotterdam and listed in the Trade Register of the Chamber of Commerce under file number 24277249) and forms the part of Openprovider General Terms and Conditions and any other agreements between you and Openprovider (collectively, the "Agreement"). Openprovider and Client are referred to herein, individually, as a "Party", and collectively as the "Parties". This DPA is effective as of the effective date of the Agreement ("Effective Date") and governs all Processing of Client Personal Data under the Agreement.

1. Definitions. Unless otherwise defined in applicable Data Protection Laws (as defined below), the capitalized terms listed in this Section have the following meanings:

1.1 "Affiliate" means any entity that controls or is under common control with a Party. "Control" means direct or indirect ownership or control of fifty percent (50%) or more of the voting interests of an entity.

1.2. "Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of processing Client Personal Data under the Agreement.

1.3 "Client Personal Data" means any Personal Data (as defined below) processed by Openprovider on Client's behalf in connection with Client's use of the Services. Client Personal Data does not include Openprovider Data.

1.4 "Data Protection Law" means any law or regulation applicable to processing of Client Personal Data under the Agreement.

1.5 "Data Subject" means an identified or identifiable natural person to whom specific Personal Data relates.

1.6 "De-Identified Data" means data that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a specific Data Subject.

1.7 "Openprovider Data" means (a) all information relating to Openprovider's business and delivery of the Services, including but not limited to Personal Data concerning Client and its employees or representatives, (b) other data concerning or relating to Client's account, transaction history, use of the Services and identity verification, and (c) subject to any restrictions under any applicable Data Protection Laws, De-Identified Data.

1.8 "Personal Data" means information that relates to an identified or identifiable natural person, including any information defined as Personal Data, Personal Information, or Personally

Identifiable Information ("PII") in any applicable Data Protection Laws. Personal Data does not include De-Identified Data.

1.9 "Processor" means a natural or legal person, public authority, agency, or body that processes Client Personal Data on behalf of a Controller under the Agreement.

1.10 "Processing" means any operation performed on Client Personal Data, such as collection, use, storage, disclosure, analysis, deletion, or modification, whether by manual or automated means.

1.11 "Sensitive Personal Data" means (a) social security number, passport number, driver's license number, or similar identifier; (b) credit or debit card information, financial information, bank account numbers, or account passwords; (c) employment, financial, genetic, biometric, or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or orientation; (e) account passwords, mother's maiden name, date of birth, and other similar information used to authenticate a user's identity; (f) criminal history; (g) biometric data used to identify a specific person (e.g., fingerprints); or (h) any other information or combination of information that falls within the definitions of "special categories of data" under any applicable Data Protection Law.

1.12 "Services" means the products or services that Openprovider has agreed to provide pursuant to the Agreement that involve processing of Client Personal Data.

1.13 "Subprocessor" means any natural or legal person, public authority, agency, or body with whom Openprovider contracts to process Client Personal Data.

1.14 "Transfer" means (a) transfer of Client Personal Data from Controller to Processor, whether by physical transfer or by granting access to Client Personal Data held or otherwise controlled by Controller or (b) an onward transfer of Client Personal Data from a Processor to a Subprocessor (and any subsequent onward transfer by a Subprocessor to another Subprocessor).

2. Scope of Data Processing and Relationship of Parties

2.1 Client as Controller or Processor

2.1.1 Where Client is a Controller, Client (a) is solely responsible for determining the purposes and means of processing Client Personal Data, (b) has all necessary authority, grounds, rights, and permissions to provide Client Personal Data to Openprovider, and (c) will comply with its obligations as a Controller under applicable Data Protection Laws.

2.1.2 Where Client is a Processor, Client (a) is solely responsible for complying with its agreement(s) with the data Controller(s) on whose behalf Client is processing Client Personal Data; (b) has all necessary permissions from the Controller to provide Client Personal Data to

Openprovider, and (c) will comply with its obligations as a Processor under applicable Data Processing Laws.

2.1.3 Client expressly acknowledges that Openprovider is not responsible for determining which laws or regulations are applicable to Client's business. Client is solely responsible for determining that the Services provided by Openprovider and the terms of the Agreement and this DPA meet Client's business, contractual, and legal obligations. Client also will ensure that Client's Processing instructions to Openprovider do not violate any applicable Data Protection Laws.

2.2 Openprovider as Processor or Subprocessor.

2.2.1 Openprovider will take all steps reasonably necessary to enable Client to comply with Client's obligations as a Controller and/or Processor under the Data Protection Laws consistent with the character, nature, scope, and purpose of the Services provided by Openprovider. For the avoidance of doubt, Openprovider is not required to undertake any steps to alter or make Openprovider's Services compliant for Client's specific use. Client's sole remedy in the event the Services are determined to be not compliant for Client's specific use is termination of any portion of the Agreement that relates to processing of Client Personal Data.

2.2.2 Openprovider will process Client Personal Data only upon documented instructions for the limited and specific purposes described in the Agreement, this DPA, or as required by law.

2.2.3 Openprovider will not sell, retain, use, or disclose Client Personal Data for a commercial purpose other than providing the Services.

2.2.4 Openprovider will not Process Client Personal Data outside of the Parties' direct business relationship described in the Agreement and this DPA.

2.2.5 Openprovider will not combine Client Personal Data with any other data Openprovider collects (directly or via any third party) other than as expressly permitted under the Agreement.

2.2.6 Openprovider will stop all Processing and will notify Client within three (3) business days if Openprovider: (a) believes that a Client instruction violates any applicable Data Processing Laws or (b) determines Openprovider is unable to comply with any applicable Data Processing Laws or its obligations under this DPA.

2.3 Affiliates.

2.3.1 Client Affiliates. For purposes of this DPA, any Personal Data provided to Openprovider or Openprovider's Affiliates by a Client Affiliate for processing on Client's and/or Client's Affiliate's behalf shall be deemed to be Client Personal Data and to have been provided by Client. Client represents that it will take all measures reasonably necessary to ensure its Affiliates comply with all Client obligations with respect to this DPA. Client is responsible for its Affiliates' compliance with all terms of this DPA.

2.3.2 Openprovider Affiliates. For purposes of this DPA, any Client Personal Data received by Openprovider's Affiliates shall be deemed to have been received by Openprovider.

Openprovider represents that it will take all measures reasonably necessary to ensure that its Affiliates comply with Openprovider's obligations with respect to processing of Client Personal Data under this DPA. Openprovider is responsible for Openprovider's Affiliates' compliance with all terms of this DPA.

3. Openprovider's Use of Subprocessors

3.1 Client provides general authorization for Openprovider to engage subprocessors.

3.2 Openprovider maintains and makes available its current list of Subprocessors in Schedule 4 (Subprocessor List), which is incorporated into and forms part of this DPA. The Subprocessor List may be maintained electronically at the URL specified in Schedule 4. Openprovider may update the Subprocessor List in accordance with Section 3.6.

3.3 Openprovider maintains information concerning its current Subprocessors in the following Subprocessor List

3.4 Before transferring Client Personal Data to a Subprocessor, Openprovider will: (a) enter into a written agreement with the Subprocessor that is at least as protective of Client Data as this DPA; (b) conduct due diligence to confirm the Subprocessor can comply with the material terms of this DPA and the Data Protection Laws as they relate to Openprovider's processing of Client Data, including the information security requirements of Sections 5, 6, and 8, and of Schedule 2 of this DPA.

3.5 Openprovider is liable for its Subprocessors' acts and omissions, including any acts or omissions of its Subprocessors' subprocessors.

3.6 New Subprocessors; Right to Object.

3.6.1 Openprovider will exercise reasonable efforts to notify Client in writing at least sixty (60) days in advance if Openprovider intends to appoint new a Subprocessor; provided, however, that sixty (60) days' advance notice is not required and Openprovider will notify Client without undue delay after the appointment of a new Subprocessor if immediate appointment is required to maintain the security of Client Personal Data or to comply with applicable law.

3.7.2 If Client reasonably objects to a new Subprocessor, Client must notify Openprovider in writing within thirty (30) days after the Subprocessor's appointment. In Openprovider's sole discretion, Openprovider may use commercially reasonable efforts to address Client's objection. If the Parties are unable to resolve Client's objection within thirty (30) days, Client may terminate this DPA and any portion of the Agreement relating to the processing of Client Personal Data.

3.8.3 If Client does not object to a new Subprocessor within thirty (30) days of notice of Subprocessor's appointment, Client will be deemed to have accepted the new Subprocessor.

3.9.4 Notice of a new Subprocessor may be provided by updating the Subprocessor list described in Section 3.2.

3.9.5 **Permitted use.** Openprovider may engage cloud infrastructure providers, software-as-a-service providers, artificial intelligence service providers, communications providers, identity-verification providers, security providers and other third-party service providers as Subprocessors where reasonably necessary to provide, secure, support or improve the Services, subject to this Section 3.

3.9.6 Prior assessment. Before permitting a Subprocessor to Process Client Personal Data, Openprovider will conduct and document a risk-based assessment appropriate to the nature, scope, context and purposes of the Processing. Such assessment will consider, where relevant:

- (a) the categories, volume and sensitivity of Client Personal Data;
- (b) the location of Processing and storage;
- (c) the Subprocessor's security, confidentiality, retention and deletion practices;
- (d) the Subprocessor's use of further subprocessors;
- (e) the Subprocessor's international-transfer mechanisms;
- (f) the Subprocessor's ability to assist Openprovider with Data Subject Requests, Security Incidents, audits, deletion and regulatory enquiries; and
- (g) in the case of artificial intelligence services, the provider's practices concerning model training, service improvement, prompt and output retention, human review and automated decision-making.

3.9.7 **Contractual requirements.** Openprovider will enter into a written agreement with each Subprocessor that imposes data protection obligations no less protective than those applicable to Openprovider under this DPA, to the extent relevant to the services performed by that Subprocessor. The agreement will require the Subprocessor to:

- (a) Process Client Personal Data only on documented instructions and only for the purposes of providing the contracted services;
- (b) ensure that persons authorised to Process Client Personal Data are subject to confidentiality obligations;
- (c) implement appropriate technical and organisational security measures;

- (d) notify Openprovider without undue delay of any Security Incident affecting Client Personal Data;
- (e) assist Openprovider in responding to Data Subject Requests and regulatory enquiries;
- (f) return or delete Client Personal Data following termination of the relevant services, except where retention is required by law;
- (g) impose equivalent obligations on any further subprocessor; and
- (h) comply with applicable international-transfer requirements.

3.9.8 Artificial intelligence services

Where a Subprocessor provides a generative artificial intelligence, machine-learning or comparable automated service, Openprovider will ensure, through contractual terms, technical configuration or other appropriate measures, that:

- (a) Client Personal Data submitted through the service is not used to train or improve general-purpose models for the benefit of the provider or unrelated third parties, unless expressly authorised by Client and permitted under applicable Data Protection Laws;
- (b) the provider does not sell Client Personal Data or use it for advertising, profiling or purposes unrelated to providing the contracted service;
- (c) retention of prompts, inputs, files, outputs and related metadata is limited to the period necessary to provide and secure the service or comply with applicable law;
- (d) human access to Client Personal Data is restricted to authorised personnel with a documented need to know, including for support, security, abuse prevention or legal compliance;
- (e) available zero-retention, regional-processing, encryption and access-control settings are used where proportionate to the nature and sensitivity of the Processing;
- (f) Sensitive Personal Data is not submitted unless the use has been specifically approved following an appropriate legal and security assessment; and
- (g) outputs are subject to appropriate human review where they are used to make decisions that may produce legal or similarly significant effects on individuals.

This wording is particularly relevant for Anthropic. Anthropic states that its commercial DPA, including SCCs, is automatically incorporated into its Commercial Terms. It also states that, for commercial services, the customer acts as controller, Anthropic acts as processor and commercial customer data is not used to train its generative models. Those protections should nevertheless be verified against the specific product and contracting route used by

Openprovider, particularly where Claude is accessed through AWS, Google Cloud or another intermediary.

4. Legal Process and Other Third Party Requests for Client Personal Data

4.1 Openprovider will not respond to any informal request for any Client Personal Data from a government body, law enforcement agency, or other person except in response to a subpoena, search warrant, court order, or other similar legal process (collectively, "Legal Process"), unless such disclosure is determined by Openprovider in its reasonable discretion to be (a) required by law, (b) necessary to protect Openprovider's systems or data from harm or misuse, or (c) necessary to protect Openprovider or any other person from damage or physical harm.

4.2 Unless prohibited by law, Openprovider will notify Client promptly if it receives any Legal Process that requires Openprovider to provide access to or disclose Client Personal Data.

4.3 Unless otherwise required by law, Openprovider will cooperate with Client (at Client's reasonable expense) in any efforts by Client to prevent disclosure of Client Personal Data in response to Legal Process.

4.4 Government and Law-Enforcement Requests

Where Openprovider or a Subprocessor receives a legally binding request from a public authority for Client Personal Data, it will, to the extent legally permitted: (a) promptly notify Client and provide available information concerning the request; (b) review the legality, scope, jurisdiction and proportionality of the request; (c) challenge the request where there are reasonable grounds to consider it unlawful, excessive or inconsistent with applicable transfer safeguards; (d) seek a waiver of any prohibition against notifying Client; (e) disclose only the minimum Personal Data legally required; (f) document the request, assessment, response and data disclosed; and (g) provide periodic aggregate information concerning government requests where legally permitted. Neither Openprovider nor its Subprocessors will provide public authorities with voluntary, direct or unrestricted access to Client Personal Data, encryption keys or systems used to Process Client Personal Data, except where expressly authorised by Client or required by applicable law.

5. Data Security

5.1 Openprovider maintains an information security program that includes appropriate and documented technical and organizational measures to ensure a level of security appropriate to the risk of Processing Client Personal Data under the Agreement, including any specific measures required by applicable Data Protection Laws.

5.2 Client expressly acknowledges that Openprovider provides security features and functionality that Client can use to protect Client Personal Data. Client is solely responsible for taking appropriate risk-based steps to protect the security of Client's account and Client Personal Data within Client's control, including by using security features and functionality

provided by Openprovider. Client also is solely responsible for ensuring that all content that Client places or causes to be placed within the Services is free of vulnerabilities that could result in the compromise of Client Personal Data and Openprovider's systems, including but not limited to malicious software. Openprovider is not responsible for backing up Client Personal Data.

5.3 KYC and Identity Verification Data. Openprovider will apply access controls, encryption or equivalent safeguards, purpose limitation, and data minimisation to identity documents, facial images, biometric comparison outputs, and other identity-verification data. Such data will be accessible only to personnel and Subprocessors with a need to know for verification, fraud prevention, support, security, legal, or compliance purposes. Openprovider will not use such data to build general-purpose biometric profiles, for advertising, or for purposes unrelated to the Services. Retention and deletion will be governed by Schedule 1 and Section 10.8.

5.4 Service Availability. Availability, uptime, maintenance windows, service credits and other service-level commitments, if any, are governed exclusively by the service level agreement, service description or other availability terms expressly incorporated into the Agreement or published by Openprovider for the relevant Service, as updated in accordance with the Agreement. This DPA does not create any separate availability warranty, uptime commitment, service credit or remedy. Openprovider will maintain commercially reasonable business continuity and resiliency measures appropriate to the nature and risk of the Processing, as further described in Schedule 2.

6. Data Security Incidents

6.1 Openprovider offers Client extensive opportunities to access and control Client Personal Data Processed on Client's behalf. Openprovider is not responsible for any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data that does not result from a compromise of Openprovider's systems. Examples of Security Incidents for which Openprovider is not responsible include Client's failure to maintain the secrecy of its passwords, downloading of malicious content, or any other security vulnerability caused by or introduced into the Services and Client's hosted environment by Client.

6.2 Openprovider will notify Client without undue delay and, in any event, no later than seventy-two (72) hours after becoming aware of a Security Incident affecting Client Personal Data. Where all relevant information is not available at the time of the initial notice, Openprovider may provide the information in phases without undue further delay. The notification obligation in this Section applies only to the extent the Security Incident concerns Client Personal Data Processed by Openprovider under this DPA.

6.3 Openprovider will use commercially reasonable efforts to notify Client of a breach of security of Openprovider's systems leading to the accidental or unlawful, destruction, loss, alteration, unauthorized disclosure of, or access to Client Personal Data ("Security Incident") within the time period required under applicable law.

6.4 Openprovider will take appropriate, risk-based steps that are reasonably necessary to contain, mitigate, and remediate a Security Incident without unreasonable delay.

6.5 Openprovider will provide information reasonably requested by Client to assess the impact of a Security Incident on Client Personal Data and for Client to provide notice of the Security Incident to governmental authorities, affected Data Subjects, or any other person.

6.6 Openprovider's acknowledgement of a Security Incident or decision to notify Client of a Security Incident is not an admission of fault or liability.

6.7 Openprovider will maintain an internal incident response and escalation process designed to ensure that suspected Security Incidents are promptly assessed and, where applicable, escalated to Openprovider's privacy, security, and legal functions. Notices under Section 6.2 will, to the extent reasonably available, describe the nature of the Security Incident, the categories and approximate number of affected Data Subjects and records, the likely consequences, and the measures taken or proposed to address and mitigate the Security Incident.

7. Data Subject Rights

7.1 Client is solely responsible for responding to any request to exercise a Data Subject's rights under the Data Protection Laws, Client's privacy policies, or Client's terms of service, including but not limited to requests to know, access, correct, or delete Client Personal Data ("Data Subject Requests").

7.2 Openprovider will not respond to a Data Subject Request except on documented instructions from Client or as otherwise required under applicable law.

7.3 Openprovider will notify Client of any Data Subject Request. Client is solely responsible for responding to any Data Subject request. If Client has exhausted all means available to respond to a Data Subject Request – subject to Client's agreement to pay Openprovider's reasonable expenses in advance – Openprovider will provide Client with assistance reasonably necessary to allow Client to respond to a Data Subject Request.

7.4 Data Portability and Export. Taking into account the nature of the Processing and the functionality of the Services, Openprovider will provide Client with reasonable means to access or export Client Personal Data in a structured, commonly used and machine-readable format where required for Client to respond to a valid request under Article 20 GDPR or equivalent applicable Data Protection Law. Openprovider's obligation is limited to Client Personal Data processed on Client's behalf that is available within the Services or can be exported using Openprovider's standard tools and processes. Openprovider is not required to create new interoperability tools, disclose confidential system information, provide data that adversely affects the rights and freedoms of others, or export data that Openprovider is legally required to retain. Any additional assistance requested by Client will be subject to technical feasibility and reimbursement of Openprovider's reasonable costs, unless applicable law requires otherwise.

8. Data Protection Impact Assessments, Prior Consultation, and Compliance Inquiries

8.1 Data Protection Impact Assessments; Prior Consultation. At Client's expense, Openprovider will provide reasonable assistance to Client in conducting any data protection impact assessments and consultations with government authorities or regulators concerning processing of Client Personal Data.

8.2 Compliance Information and Audits. Upon Client's reasonable written request, Openprovider will make available information reasonably necessary to demonstrate compliance with Article 28 of the GDPR and the corresponding requirements of other applicable Data Protection Laws, which may include relevant third-party certifications, audit summaries, penetration-test summaries, or other independent assurance reports, subject to confidentiality, security, and legal restrictions. If such information is not reasonably sufficient to address a substantiated compliance concern, Client may request an audit in accordance with Section 8.3.

8.3 Any audit requested by Client must: (a) be limited to Processing of Client Personal Data under this DPA; (b) be conducted no more than once in any twelve (12)-month period, unless required by a competent supervisory authority or following a material Security Incident affecting Client Personal Data; (c) be conducted by Client or an independent auditor that is not a competitor of Openprovider and is bound by written confidentiality obligations; (d) take place during normal business hours on at least thirty (30) days' prior written notice; (e) avoid access to data of other customers and avoid unreasonable disruption to Openprovider's business, systems, security, or personnel; and (f) be at Client's cost. Openprovider may satisfy an audit request through a remote review or independent third-party audit report where reasonably appropriate. Openprovider may charge its reasonable costs for assistance beyond the information ordinarily made available under Section 8.2.

9. Jurisdiction Specific Requirements and International Transfers of Personal Data

9.1 General Requirement. Openprovider will not transfer Client Personal Data to a recipient located outside the country or region in which the Personal Data is protected unless the Transfer complies with applicable Data Protection Laws.

9.2 Transfer Mechanisms. Where Client Personal Data protected by the GDPR is Transferred outside the EEA, the Transfer will be based on one or more of the following, as applicable: (a) an adequacy decision under Article 45 GDPR; (b) the EU-US Data Privacy Framework, but only where the relevant US recipient is actively certified, the certification covers the relevant data and service, and the framework remains legally valid; (c) the EU Standard Contractual Clauses adopted under Commission Implementing Decision (EU) 2021/914; (d) binding corporate rules approved under Article 47 GDPR; or (e) another lawful transfer mechanism available under Chapter V GDPR.

9.3 Verification of Transfer Mechanism. Before relying on an adequacy framework or certification mechanism, Openprovider will verify that the relevant recipient, service and category of Personal Data fall within the scope of that mechanism. Openprovider will not represent that it or a Subprocessor participates in a certification framework unless that participation has been verified and remains current.

9.4 UK and Swiss Transfers. Transfers of Personal Data protected by UK or Swiss data protection law will be subject to the transfer mechanism required by the relevant law, including, where applicable, the UK International Data Transfer Agreement, the UK Addendum to the EU SCCs, recognised adequacy regulations or the Swiss adaptations to the EU SCCs.

9.5 Transfer Impact Assessments. Before making a Transfer in reliance on the EU SCCs or another mechanism requiring an assessment of third-country protection, Openprovider will conduct and document a transfer impact assessment proportionate to the circumstances of the Transfer. The assessment may consider the nature, sensitivity and volume of the Personal Data; the purposes and frequency of the Transfer; the identity, location and role of the importer and onward recipients; applicable laws and practices concerning government access and redress; the importer's documented experience of government-access requests where lawfully available; and the contractual, technical and organisational safeguards applied.

9.6 Reassessment and Cooperation. Each relevant data importer and Subprocessor will provide information reasonably necessary for Openprovider to complete and update the transfer impact assessment. Openprovider will reassess the Transfer where it becomes aware of a material change in the destination country's laws or practices, the Processing, the recipient, the onward-transfer chain or the validity of the transfer mechanism.

9.7 Supplementary Measures. Where reasonably necessary to ensure an essentially equivalent level of protection, Openprovider will implement supplementary safeguards, which may include encryption in transit and at rest; retention of encryption keys within the EEA or under the control of Openprovider or Client where technically feasible; pseudonymisation or tokenisation; data minimisation; regional processing and storage controls; role-based access controls, multi-factor authentication and logging; contractual restrictions on government disclosures and onward Transfers; transparency reporting; and suspension or termination of the Transfer where adequate protection can no longer be maintained.

10. General

10.1 Complete Agreement; Interpretation. This DPA constitutes the entire agreement between the Parties concerning the subject matter of this DPA and supersedes all prior or contemporaneous representations, understandings, agreements, and communications between the Parties, whether written or verbal, regarding the subject matter of this DPA. In the event of a conflict between this DPA and the Agreement (or any other agreement between the Parties), this DPA will govern and control with respect to the subject matter of this DPA. If there is a conflict between any terms of this DPA and the Mandatory Transfer Provisions described in Schedule 3, those Mandatory Transfer Provisions shall prevail.

10.2 Amendment. This DPA may be modified or amended by Openprovider in its sole discretion pursuant to the procedures set forth in the Agreement. If Client disagrees with such amendment, Client's sole remedy is to terminate that portion of the Agreement relating to the Processing of Client Personal Data on thirty (30) days' notice. Unless expressly agreed by the

Parties in writing, any amendment of this Agreement is effective only with respect to Processing that occurs after the date of such amendment.

10.3 Waiver. The waiver of any breach of this DPA is effective only if in writing by an authorized representative of the Party waiving such breach and no such waiver will be construed as a waiver of any subsequent breach.

10.4 Severance. If any provision of this DPA is found to be unenforceable, then that provision shall be modified to the extent necessary to make it enforceable and the remainder of this DPA shall remain in effect as written. However, if modifying any unenforceable provision would result the failure of the essential purpose of this DPA, the entire DPA shall be considered null and void unless amended pursuant to Section 10.2.

10.5 Notices. Except as expressly stated herein, notices required under this DPA will be provided in accordance with the Notice requirements set forth in the Agreement.

10.6 Liability. Except to the extent prohibited by applicable law, each Party's liability arising out of or in connection with this DPA, including any Security Incident or breach of applicable Data Protection Laws, is subject to the exclusions, limitations and procedures set out in the Agreement. Notwithstanding any lower general monetary cap in the Agreement, Openprovider's aggregate liability for all claims arising under this DPA in any twelve (12)-month period will not exceed the greater of (a) EUR 100,000 and (b) two (2) times the fees paid or payable by Client for the affected Services during the twelve (12) months immediately preceding the event giving rise to the claim. This separate cap is aggregate and not per claim, Data Subject, Security Incident or affected record. It does not apply to liability that cannot lawfully be limited or excluded. Neither Party is liable to the other for regulatory fines or penalties imposed directly on the other Party to the extent such fines or penalties arise from that other Party's acts, omissions, instructions or failure to comply with applicable law.

10.7 Enforcement. The terms of this DPA may only be enforced by the Parties on behalf of themselves and their respective Affiliates in accordance with the dispute resolution provisions set forth in the Agreement. This restriction on enforcement has no effect, however, on an individual Data Subject's ability to enforce their rights under the Data Protection Laws.

10.8 Termination; Return and Deletion. Unless terminated earlier pursuant to the Agreement, this DPA will terminate when Openprovider completes the Processing of Client Personal Data or the Agreement terminates, whichever occurs later. Following termination and upon Client's written request, Openprovider will, at Client's choice and to the extent technically feasible, return or delete Client Personal Data within sixty (60) days, except to the extent retention is required or permitted by applicable law, binding registry or registrar obligations, legal process, the establishment, exercise or defence of legal claims, or Openprovider's documented retention policies. Client Personal Data contained in backups will be deleted or rendered inaccessible in accordance with Openprovider's ordinary backup rotation cycle and will remain protected under this DPA until deletion. Upon Client's written request, Openprovider will provide written confirmation, signed or issued by an authorised representative, that deletion required under this Section has been completed, subject to the foregoing retention exceptions. Any retained Client Personal

Data will be isolated from further active Processing except for the purpose requiring its retention and will be deleted when that purpose ceases to apply.

10.9 Governing Law and Jurisdiction. Except as expressly provided in Section 10.9.1, this DPA and any non-contractual obligations arising out of or in connection with it are governed by the governing law and subject to the jurisdiction specified in the Agreement. Mandatory provisions of applicable Data Protection Laws remain unaffected.

10.9.1 Mandatory Transfer Mechanisms. The choice of law, forum and supervisory authority specified in Schedule 3 apply solely to the interpretation and enforcement of the applicable Standard Contractual Clauses or other Mandatory Transfer Mechanism, and only to the extent required by that mechanism. They do not replace or amend the governing law or jurisdiction applicable to the Agreement or the remainder of this DPA. Accordingly, the reference to German law and German courts in Sections 4.2.4 and 4.2.5 of Schedule 3 applies only to disputes arising under the EU Standard Contractual Clauses.

Schedule 1: Details of Processing of Client Personal Data

This Schedule 1 includes details of Processing Client Personal Data Required under the Data Protection Laws.

Subject matter and duration of Processing of Client Personal Data:

The subject matter of the Processing is the provision, administration, security, support, billing, compliance, and improvement of the Services described in the Agreement, including domain name registration and lifecycle management, reseller account administration, technical support, fraud prevention, sanctions screening, identity verification, and compliance with applicable registrar, registry, legal, and regulatory requirements. Processing continues for the term of the Agreement and thereafter only for the retention periods specified below.

The nature and purpose of Processing of Client Personal Data:

Openprovider Processes Client Personal Data to provide and secure the Services; create and administer accounts; register, renew, transfer, restore, suspend, and manage domain names; communicate with Client, registrants, registries, registrars, service providers, authorities, and dispute-resolution providers; process payments and maintain transaction records; provide support; verify identity and authority; prevent fraud, abuse, and unlawful activity; comply with contractual, registry, ICANN, legal, and regulatory obligations; and establish, exercise, or defend legal claims. Processing operations may include collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, transmission, disclosure, restriction, matching, erasure, and destruction, by manual or automated means as appropriate to the Services.

Type of Personal Data and Categories of Data Subjects:

Categories of Data Subjects may include Client's and its customers' or resellers' registrants; administrative, technical, billing, and abuse contacts; account users; authorised representatives; beneficial owners, directors, and officers; payers and payment contacts; support requestors; complainants; and other individuals whose Personal Data is submitted to or generated through the Services. Categories of Client Personal Data may include: names; organisation and job-title information; postal and billing addresses; email addresses; telephone numbers; account identifiers; usernames; authentication and access data; IP addresses; device and log data; API and transaction records; domain registration and lifecycle data; registration data directory or WHOIS/RDAP data; registry and registrar identifiers; payment and invoicing information; communications and support content; abuse, complaint, dispute, and legal-process records; sanctions and fraud-screening results; and identity-verification data, including copies of identity documents, facial images, liveness or similarity results, and related verification metadata where required for the Services.

Sensitive Data or Special Categories of Data:

Sensitive Personal Data is not required for ordinary use of the Services except where identity verification, regulatory compliance, fraud prevention, or a specific registry requirement necessitates it. Where such data is Processed, it may include government-issued identification numbers and documents, date of birth, financial account information, and biometric data used solely to verify identity. Client will not submit other special categories of Personal Data unless expressly agreed in writing and lawfully permitted.

Obligations and Rights of the Controller:

Retention Periods:

- a. Domain registration and registration-data records: retained for the active registration and account lifecycle and, where the ICANN Registrar Accreditation Agreement or an applicable registry policy applies, for at least two (2) years following expiration, deletion, transfer, or termination of the relevant registration or relationship, or for any longer period required by applicable law, registry policy, legal hold, or the establishment, exercise, or defence of legal claims.
- b. KYC and identity-verification data: copies of identity documents, facial images, and comparable verification inputs will ordinarily be deleted or irreversibly anonymised within thirty (30) days after completion of the verification process, unless a longer period is required by applicable law, a registry or authority, fraud-prevention needs supported by applicable law, an unresolved dispute, or a legal hold. Openprovider may retain the verification outcome, audit trail, reference number, and minimum evidence necessary to demonstrate that verification was completed for the applicable statutory or contractual retention period. Openprovider will not retain biometric templates for independent reuse or identification unless expressly required by applicable law or the relevant verification service and disclosed to Client.
- c. Account, support, security, transaction, billing, and compliance records: retained for the term of the Agreement and thereafter for the period reasonably necessary under Openprovider's documented data retention policy, applicable accounting and tax laws, security and fraud-prevention requirements, contractual limitation periods, and legal or regulatory obligations.
- d. Deletion following termination: subject to the exceptions above, Client Personal Data will be returned, deleted, or de-identified in accordance with Section 10.8. Where several retention rules apply, the longest applicable mandatory or defensible retention period will govern. Openprovider's current privacy and retention information is available at <https://www.openprovider.com/legal/privacy-policy>.

ICANN and Registry Retention Requirements. Notwithstanding any shorter period stated in this DPA, Openprovider may retain registration data, transaction records, communications and other records for the periods required by the ICANN Registrar Accreditation Agreement, applicable ICANN Consensus Policies, registry agreements, registry policies, law-enforcement preservation requests, tax or accounting laws, or other applicable legal or regulatory obligations. Where the ICANN Registrar Accreditation Agreement requires retention of registration data, Openprovider may retain the relevant data for two (2) years following the expiry, cancellation, transfer or termination of the applicable domain name registration or registrar sponsorship, as applicable. Any data retained under this paragraph will be isolated or access-restricted where reasonably practicable, processed solely for the applicable legal, compliance, dispute-resolution, fraud-prevention or security purpose, and deleted or de-identified when the applicable retention obligation expires, unless a further lawful basis requires continued retention.

The obligations and rights of Client are described in the Agreement and this DPA.

Schedule 2: Technical and Organizational Security Measures

Openprovider will implement and maintain the following specific technical and organizational measures to protect Client Personal Data.

1. Applicability

1.1 The requirements of this Schedule 2 apply to Openprovider and any Subprocessor (including but not limited to any cloud service provider) used by Openprovider to provide the Services and/or Process Client Personal Data.

1.2 If Openprovider uses any Subprocessor to provide the Services and/or Process Client Personal Data, Openprovider shall ensure that such Subprocessor complies with each of the requirements of this Schedule.

2. Information Privacy and Data Security Management

2.1 Risk Management Process. Openprovider shall maintain an appropriate risk management process to frame, assess, respond to and monitor risk to Client Personal Data, consistent with Openprovider's obligations under the Agreement, the DPA, and applicable law.

2.2 Information Security Program Scope. At a minimum, Openprovider's information security program, including all applicable privacy and data protection policies, shall be designed to:

2.2.1 Protect the confidentiality, integrity and availability of Client Personal Data in Openprovider's possession or control or to which Openprovider has access; and

2.2.2 Protect against reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of Client Personal Data.

2.3 Information Security Program Updates. Openprovider will regularly review and update its information security program in accordance with industry standard practices and frameworks appropriate to the type, volume, and sensitivity of Client Personal Data processed by Openprovider.

2.4 Risk Assessments and Testing. Openprovider will regularly conduct risk assessments for all systems processing Client Personal Data and will periodically conduct third-party penetration testing on applications and infrastructure used to provide the Services as reasonably deemed necessary by Openprovider.

2.5 Continuity and Resiliency. Openprovider will implement appropriate measures to protect the integrity and availability of its systems that process Client Personal Data.

4. Security Operations

4.1 Secure System Configuration. Openprovider will establish controls to ensure that systems used to provide the Services and/or Process Client Personal Data are securely configured.

4.2 Vulnerability and Patch Management. Openprovider will establish and maintain a vulnerability and patch management system that ensures all systems used to provide the Services and/or Process Client Personal Data are patched against known security vulnerabilities in a reasonable time period based on the criticality of the patch and sensitivity of the Client Personal Data.

4.3 Malware Prevention. Openprovider will implement detection, prevention, and remediation controls to protect against malicious software (including appropriate user awareness programs).

4.4 Logging and Auditing. Openprovider will employ a log management program that defines the scope, creation, storage, analysis, and disposal of logs using risk-based industry standards.

4.5 Security Incident Detection and Response. Openprovider will maintain risk-based systems for detecting Security Incidents as required by Section 6 of the Agreement, including use of intrusion detection and intrusion prevention systems.

5. Training

Openprovider will ensure that its personnel receive regular training regarding their confidentiality and data protection obligations as they relate to Client Personal Data.

7. Data Security Controls

7.1 Data Segregation. Openprovider will maintain Client Personal Data in logically separate and secure environments.

7.2 Encryption and other Measures. Openprovider will employ appropriate risk-based measures to protect Client Personal Data, including encryption, pseudonymization, and other appropriate measures such as employing algorithms for hashing secrets, including passwords and API tokens used for accessing systems containing Client Personal Data.

2. European Union/European Economic Area

2.1 Subprocessors

2.1.1 When Openprovider engages a Subprocessor, it will:

2.1.1.1 Require the Subprocessor to comply with those technical and organizational measures set forth in Sections 5, 6, and 8 of the DPA, and Schedule 2 of the DPA that are appropriate to the nature of processing by the Subprocessor, including but not limited to all technical and

organizational measures required by Article 28 of the EU General Data Protection Regulation (“GDPR”); and

2.1.1.2 Require the Subprocessor to agree in writing to only process Client Personal Data (a) in the EU/EEA, (b) in a country that the European Commission has declared to have an “adequate” level of data protection, or (c) on terms set forth in Schedule 3 regarding international Transfers of Client Personal Data.

2.2 Liability for Regulatory Penalties. Notwithstanding any other term set forth in this DPA or the Agreement (including either Party’s indemnification obligations under the Agreement), neither Party will be responsible for any fines issued or levied by any regulatory authority or government body on the other Party, including any fines under Article 83 of the EU GDPR.

Schedule 3: International Mandatory Cross Border Transfer Mechanisms

1. Definitions

1.1 The “Data Privacy Framework (‘DPF’)” means the EU-US, Swiss-US, or UK-US Data Privacy Framework certification programs operated by the U.S. Department of Commerce (<https://www.dataprivacyframework.gov>).

1.2 The “UK-US Data Bridge” means the UK Extension to the EU-US Data Privacy Framework.

1.3 The “EU Standard Contractual Clauses” mean the standard contractual clauses approved by the European Commission under Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.4 The UK International Data Transfer Agreement (“UK IDTA”) issued by the UK Information Commissioner, Version B1.0, is deemed to be executed by the Parties as of the Effective Date of the Agreement, and the EU Standard Contractual Clauses are deemed amended as specified by the UK IDTA in relation to data transfers from the UK.

2. Order of Precedence

2.1 No Mandatory Transfer Mechanism is used if a transfer is made to a country that has been deemed to offer an adequate level of data protection by the Data Protection Laws of the country from which such Client Personal Data is transferred.

2.2 If a Transfer is required and such Transfer is covered by more than one Mandatory Transfer Mechanism, the Transfer will be subject to a single Mandatory Transfer Mechanism in accordance with the following order of precedence: (a) the applicable EU or Swiss DPF; (b) the UK-US Data Bridge; (c) the EU Standard Contractual Clauses; (d) the UK IDTA; or (e) any other applicable Mandatory Transfer Mechanism permitted under the applicable Data Protection Law.

2.3 If a Mandatory Transfer Mechanism is deemed invalid after execution of this Agreement, all future Transfers will be deemed made by the next applicable valid Mandatory Transfer Mechanism.

3. Data Privacy Framework

3.1 Self-Certification.

3.1.1 Reliance on the DPF. The DPF may be relied upon only where the relevant US data importer is actively certified, the certification covers the relevant service and category of Personal Data, and the DPF remains a valid transfer mechanism. Openprovider will verify the recipient’s certification status before reliance and periodically thereafter.

3.2 Status

3.2.1 EU-US DPF. The EU-US DPF has been deemed to provide an adequate level of data protection by the European Commission pursuant to a 10 July 2023 adequacy decision and is in effect as of 10 October 2023.

3.2.2 UK-US Data Bridge. The UK-US Data Bridge has been deemed to provide an adequate level of data protection by the UK Secretary of State for Science, Innovation, and Technology who has laid adequacy regulations in Parliament as of 21 September 2023. The UK-US Data Bridge regulations went into effect on 12 October 2023.

3.2.3 Swiss-US DPF. The Swiss-US DPF has been approved by the Swiss Federal Council and is in effect as of 15 September 2024.

3.3 Company and Company's Subprocessors will take all steps necessary to enable Openprovider to comply with its obligations as a Controller and/or Processor under the DPF, including but not limited to assisting Openprovider and/or the Controller in responding to requests from individuals to exercise their Data Subject rights.

4. The EU Standard Contractual Clauses

4.1 Incorporation. Where required, the EU Standard Contractual Clauses are incorporated into this DPA by reference and are deemed executed by the relevant data exporter and data importer.

4.2 Applicable Module. The applicable module is determined according to the parties' roles: Module One for Controller-to-Controller Transfers; Module Two for Controller-to-Processor Transfers; Module Three for Processor-to-Processor Transfers; and Module Four for Processor-to-Controller Transfers. Where Openprovider engages a Subprocessor outside the EEA to Process Client Personal Data on behalf of Client, Module Three will ordinarily apply. Where Openprovider Transfers Personal Data for which it acts as Controller to a service provider acting as Processor, Module Two will ordinarily apply.

4.3 SCC Selections. Clause 7, the optional docking clause, will apply. Under Clause 9, Option 2, general written authorisation will apply with the notice period set out in Section 3. The optional language in Clause 11 will not apply. For Clause 17, Option 1, the SCCs will be governed by the laws of the Netherlands. For Clause 18(b), disputes will be resolved before the competent courts of the Netherlands. The competent supervisory authority under Clause 13 will be determined in accordance with the SCCs and the establishment or residence of the relevant data exporter.

4.4 For purposes of Annex I, Part A:

4.4.1 Data Exporter

4.4.1.1 The Data Exporter will be Company.

4.4.1.2 Company may be contacted at the addresses set forth in the notice provision of the Agreement.

4.4.1.3 By entering into this DPA, Company is deemed to have signed these EU Standard Contractual Clauses, including their Annexes, as of the Effective Date of the Agreement.

4.4.2 Data Importer

4.4.2.1 The Data Importer will be Openprovider and/or authorized affiliates of Openprovider.

4.4.2.2 Openprovider may be contacted at the addresses set forth in the notice provision of the Agreement or at privacy@Openprovider.com.

4.4.2.3 By entering into this DPA, Openprovider is deemed to have signed these EU Standard Contractual Clauses, including their Annexes, as of the Effective Date of the Agreement.

4.5 For purposes of Annex I, Part B:

4.5.1 The categories of Data Subjects are described in Schedule 1

4.5.2 The sensitive data (if any) Transferred is described in Schedule 1.

4.5.3 The frequency of Transfer is the duration of the Agreement and DPA.

4.5.4 The nature of Processing is described in Schedule 1.

4.5.5 The purpose of Processing is described in Schedule 1.

4.5.6 The period of Processing is described in Schedule 1.

4.6 For purposes of Annex I, Part C, in accordance with clause 13, the competent supervisory authority is defined as follows:

4.6.1 The Swiss Federal Data Protection and Information Commissioner shall act as the competent supervisory authority insofar as the relevant Transfer or Onward Transfer is governed by Swiss Data Protection Laws and Regulations.

4.7 In Annex II of the EU Standard Contractual Clauses, Schedule 2 contains the technical and organizational measures implemented by Company as Data Importer under the DPA.

4.8 In Annex III of the EU Standard Contractual Clauses, view a list of Company's Subprocessors.

Schedule 4: Subprocessor List

The current Subprocessor List is incorporated into this DPA and will identify, at a minimum, each Subprocessor's legal name, the service or processing activity performed, the location of Processing, and the applicable transfer mechanism where relevant. Openprovider may maintain the list electronically and update it in accordance with Section 3.5.

Current list URL:

•

WHMCS
Zendesk Inc.
Aircall
HotJar
Sentry
Landbot
UserGuiding
Cloudcone
HubSpot
Meta / Google Ads (paid advertising)
Vercel
Modjo
LinkedIn Sales Navigator
Twinfield
QuickBooks
SalesforceTableau
Chargify
Adyen BV
Digidentity BV
Google Workspace
Internet Escrow Services
Webflow
Typeform, S.L.
GCP
Mailgun
StatusCake
ngrok

•

Until the public URL is inserted, the current approved Subprocessor List maintained by Openprovider's Legal/Privacy function is deemed attached to and incorporated into this Schedule 4.