DIGIDATIONS DATA PROCESSING ADDENDUM

Effective date: December 1, 2026

This Data Processing Addendum ("DPA") forms part of the digiDations End User License Agreement at https://www.digidations.com/legal/eula, or any separately signed agreement for digiDations Products (the "Agreement"). It is between digiDations Pte. Ltd. (UEN 202414953N), 20 Anson Road, #06-16, Singapore 079912 ("digiDations"), and the Licensee named in the applicable Order ("Licensee").

This DPA applies where digiDations processes Customer Personal Data on Licensee's behalf in providing the Products. It is incorporated into the Agreement under Section 5.2 of the EULA and needs no separate signature. A Licensee that requires a countersigned copy may request one at legal@digidations.com.

Capitalized terms not defined in this DPA have the meanings given in the Agreement. If this DPA conflicts with the Agreement regarding the processing of Customer Personal Data, this DPA prevails. If the Standard Contractual Clauses conflict with this DPA or the Agreement, the Standard Contractual Clauses prevail.

1. Definitions

1.1. Customer Personal Data

This term means Personal Data contained in Customer Data that digiDations processes on Licensee's behalf as a Processor or, under the PDPA, as a data intermediary.

1.2. Data Protection Laws

This term means all laws that apply to the processing of Customer Personal Data under the Agreement, including, as applicable: the Singapore Personal Data Protection Act 2012 ("PDPA"); Regulation (EU) 2016/679 ("EU GDPR"); the EU GDPR as it forms part of UK law, together with the UK Data Protection Act 2018 ("UK GDPR"); the Swiss Federal Act on Data Protection ("FADP"); and the California Consumer Privacy Act, as amended ("CCPA"), and comparable US state privacy laws ("US State Privacy Laws").

1.3. Controller, Processor and Related Terms

The terms Controller, Processor, Data Subject, Personal Data, processing, and Supervisory Authority have the meanings given in the EU GDPR. They include the equivalent terms under other Data Protection Laws, such as "organisation" and "data intermediary" under the PDPA and "business," "service provider," and "personal information" under the CCPA.

1.4. Personal Data Breach

This term means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data processed by digiDations or its Subprocessors. It excludes unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, such as pings, port scans, blocked attacks, and failed log-in attempts.

1.5. Subprocessor

This term means a third party engaged by digiDations that processes Customer Personal Data. It excludes digiDations' employees and individual contractors under its direct control, and providers of facilities or infrastructure, such as colocation facilities, that have no logical access to Customer Personal Data.

1.6. Standard Contractual Clauses (SCCs)

This term means the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

1.7. UK Addendum

This term means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the UK Data Protection Act 2018, version B1.0, as amended or replaced from time to time.

1.8. Restricted Transfer

This term means a transfer of Customer Personal Data that would be prohibited by Data Protection Laws without a legally recognized transfer mechanism.

1.9. Security Measures

This term means the technical and organizational measures described in Annex 2.

1.10. EEA

This term means the European Economic Area, which comprises the member states of the European Union together with Iceland, Liechtenstein, and Norway.

2. Roles and Scope of Processing

2.1. Roles

For Customer Personal Data, Licensee is the Controller, or a Processor acting on behalf of its own Controller such as an Affiliate, and digiDations is a Processor or sub-processor. Under the PDPA, digiDations acts as a data intermediary of Licensee.

2.2. digiDations as Controller

digiDations processes Authorized User account and contact details for account administration, billing, security, support, and legal compliance, and Operational Data under Section 6.4 of the EULA, as an independent controller under its Privacy Policy at https://www.digidations.com/legal/privacy. This DPA does not apply to that processing.

2.3. Details of Processing

The subject matter, duration, nature, and purpose of the processing, and the types of Customer Personal Data and categories of Data Subjects, are described in Annex 1.

2.4. Nature of the Products

The Products are designed to discover and validate exposures in Licensee's systems. By their nature they may collect Personal Data present in those systems, such as usernames, email addresses, credential material, and content of accessed files. Licensee determines the targets, scope, and configuration of testing under Section 3.4 of the EULA, and therefore the Customer Personal Data that may be collected.

3. digiDations Obligations

3.1. Instructions

digiDations will process Customer Personal Data only on Licensee's documented instructions, unless processing is required by applicable law, in which case digiDations will inform Licensee before processing unless the law prohibits it. Licensee's instructions are the Agreement, the applicable Order, Licensee's configuration and use of the Products, and other reasonable written instructions consistent with the Agreement. Instructions outside the scope of the Agreement require mutual agreement and may incur additional fees.

3.2. Unlawful Instructions

digiDations will promptly inform Licensee if, in its opinion, an instruction infringes Data Protection Laws. digiDations is not required to perform legal analysis of Licensee's instructions.

3.3. No Other Use

digiDations will not sell Customer Personal Data, use it for its own purposes except as described in Section 2.2, or use it to train AI models, as provided in Section 6.4 of the EULA.

3.4. Personnel

digiDations will limit access to Customer Personal Data to personnel who need it to perform the Agreement, who are bound by written confidentiality obligations or an appropriate statutory duty of confidentiality, and who receive appropriate data protection and security training.

3.5. Security

digiDations will implement and maintain the Security Measures. digiDations may update the Security Measures from time to time, provided the updates do not materially reduce the overall protection of Customer Personal Data. digiDations maintains ISO/IEC 27001 certification and Cyber Trust mark certification (Advocate tier) within the scope stated in each certificate.

3.6. Records and Contact

digiDations will maintain records of its processing activities as required by Data Protection Laws. digiDations' data protection officer can be contacted at privacy@digidations.com.

4. Licensee Obligations

4.1. Lawful Basis

Licensee is responsible for having a lawful basis, and for giving any notices and obtaining any consents required by Data Protection Laws, for digiDations to process Customer Personal Data under this DPA. This includes processing that results from testing systems that contain Personal Data and from Licensee's use of AI-enabled features.

4.2. Lawful Instructions

Licensee's instructions and its configuration of the Products must comply with Data Protection Laws.

4.3. Data Minimization

Licensee will not intentionally submit special categories of Personal Data, government identification numbers, or financial account data to the Products, beyond what is incidentally present in systems within the scope of testing. Where the Products provide options to exclude targets, mask data, or limit evidence capture, Licensee is responsible for using them as appropriate.

4.4. Customer Environments

Licensee is responsible for the security of its own environments, accounts, and credentials, including environments running Customer-Hosted Software, as provided in Section 4.1 of the EULA.

4.5. Licensee as Processor

Where Licensee acts as a Processor, Licensee warrants that its instructions, including the appointment of digiDations and the authorization of Subprocessors, are authorized by the relevant Controller. Licensee is the sole point of contact for digiDations and will relay any communications with that Controller.

5. Subprocessors

5.1. Authorization

Licensee gives digiDations general written authorization to engage Subprocessors. The Subprocessors engaged at the date of this DPA are listed in Annex 3, and the current list is published at https://www.digidations.com/legal/subprocessors.

5.2. Subprocessor Terms

digiDations will engage each Subprocessor under a written contract that imposes data protection obligations no less protective than those in this DPA, to the extent relevant to the services the Subprocessor provides. digiDations remains liable for each Subprocessor's performance of those obligations.

5.3. Notice of Changes

digiDations will give at least **thirty (30) days**' notice before adding or replacing a Subprocessor that will process Licensee's Customer Personal Data, by email to Licensee's notice contact in the Order or its account administrators and by updating the published list. Where a change is urgently required for security or service continuity, digiDations will give notice promptly after the change.

5.4. Objection

Licensee may object to a new Subprocessor that will process Licensee's Customer Personal Data, on reasonable data protection grounds, by written notice within the notice period. The parties will discuss the objection in good faith, and digiDations may offer a reasonable alternative. If the objection is not resolved within **thirty (30) days**, Licensee may, by written notice, terminate the affected subscription, or the affected feature where it can be separated, and receive the refund calculated under Section 8.1 of the EULA. This is Licensee's sole remedy for an unresolved objection.

5.5. SCCs

This Section 5 constitutes Licensee's general authorization under Clause 9(a), Option 2, of the SCCs. Copies of Subprocessor agreements provided under Clause 9(c) may be redacted to remove commercial information or replaced by a summary.

6. Data Subject Requests and Assistance

6.1. Data Subject Requests

If digiDations receives a request from a Data Subject that identifies Licensee, digiDations will promptly forward it to Licensee and will not respond, other than to direct the Data Subject to Licensee, unless required by law. Taking into account the nature of the processing, digiDations will provide reasonable assistance, including through the functionality of the Products, to help Licensee respond to Data Subject requests it cannot fulfill itself.

6.2. Impact Assessments and Consultations

digiDations will provide reasonable assistance with Licensee's data protection impact assessments and prior consultations with Supervisory Authorities, taking into account the nature of the processing and the information available to digiDations. digiDations may meet this obligation first through its Documentation, certifications, and standard security information.

6.3. Government Requests

If digiDations receives a request from a public authority for access to Customer Personal Data, digiDations will, unless legally prohibited, notify Licensee promptly and redirect the authority to Licensee. digiDations will assess the lawfulness of the request, challenge it where there are reasonable grounds to consider it unlawful, and disclose only the minimum Customer Personal Data required.

6.4. Costs

Assistance under this DPA is provided on the terms in Section 5.2 of the EULA, including reasonable charges for substantial additional work except where the assistance is required by law without charge or is needed to remedy digiDations' breach.

7. Personal Data Breach

7.1. Notification

digiDations will notify Licensee of a Personal Data Breach without undue delay, and in any event within **seventy-two (72) hours** after becoming aware of it, by email to Licensee's notice contact in the Order or its account administrators.

7.2. Content

The notification will describe, to the extent known: the nature of the breach; the categories and approximate number of Data Subjects and records concerned; the likely consequences; the measures taken or proposed to address the breach and mitigate its effects; and a contact point for more information. Where information is not available at once, digiDations will provide it in phases without undue further delay.

7.3. Response

digiDations will take reasonable steps to contain, investigate, and mitigate the breach, and will cooperate reasonably with Licensee. Licensee decides whether to notify Supervisory Authorities or Data Subjects, unless the law requires digiDations to notify directly.

7.4. No Admission

Notification of, or a response to, a Personal Data Breach is not an acknowledgement of fault or liability by digiDations.

8. International Transfers

8.1. Processing Locations

digiDations hosts SaaS Customer Data in digiDations-operated infrastructure in Singapore. AI inference through the LLM service made available through digiDations runs in Amazon Bedrock in the AWS Asia Pacific (Singapore) region. Other processing locations are those listed in Annex 3, and any additional location requires notice under Section 5.3.

8.2. Transfers from Singapore

Where digiDations transfers Customer Personal Data outside Singapore, it will ensure the recipient is bound by legally enforceable obligations providing a standard of protection comparable to the PDPA, as required by section 26 of the PDPA and Part 3 of the Personal Data Protection Regulations 2021.

8.3. Transfers from the EEA

Singapore is not covered by an EU adequacy decision. For Restricted Transfers of Customer Personal Data from the EEA to digiDations, the SCCs are incorporated into this DPA by reference, with Licensee as data exporter and digiDations as data importer, completed as follows:

SCC Provision	Election
Module	Module Two (controller to processor) where Licensee is a Controller; Module Three (processor to processor) where Licensee is a Processor
Clause 7 (docking clause)	Included
Clause 9(a) (sub-processors)	Option 2, general written authorization, with notice under Section 5.3 of this DPA
Clause 11(a) (independent dispute resolution body)	Optional wording not included
Clause 13 (supervision)	The supervisory authority determined under Clause 13(a), as stated in Annex 1
Clause 17 (governing law)	Option 1, the law of Ireland
Clause 18(b) (forum)	The courts of Ireland
Annex I.A and I.B	Annex 1 of this DPA
Annex I.C	Annex 1 of this DPA
Annex II	Annex 2 of this DPA
Annex III	Annex 3 of this DPA

Audits under Clause 8.9, deletion under Clauses 8.5 and 16(d), and breach notification under Clause 8.6 are carried out as described in Sections 10, 11, and 7 of this DPA, to the extent consistent with the SCCs.

8.4. Transfers from the UK

For Restricted Transfers from the UK, the UK Addendum is incorporated into this DPA by reference. Table 1 is completed with the parties' details in Annex 1. Table 2 is completed with the SCC modules and elections in Section 8.3. Table 3 is completed with Annexes 1 to 3. For Table 4, both the importer and the exporter may end the UK Addendum as set out in its Section 19.

8.5. Transfers from Switzerland

For Restricted Transfers governed by the FADP, the SCCs apply as set out in Section 8.3 with these changes: the Swiss Federal Data Protection and Information Commissioner is the competent supervisory authority; references to the EU GDPR include the FADP; and "Member State" in Clause 18(c) includes Switzerland, so that Data Subjects in Switzerland may bring claims where they habitually reside.

8.6. Onward Transfers

digiDations will not make an onward Restricted Transfer to a Subprocessor without a transfer mechanism recognized by the applicable Data Protection Laws.

8.7. Transfer Assessments and Alternatives

digiDations will provide information Licensee reasonably requires for a transfer impact assessment. If a transfer mechanism used under this DPA is invalidated or replaced, the parties will cooperate in good faith to adopt a valid alternative.

9. US State Privacy Laws

9.1. Service Provider

To the extent the CCPA or other US State Privacy Laws apply, digiDations acts as Licensee's service provider or processor. The business purposes for which digiDations processes Customer Personal Data are providing, supporting, and securing the Products as described in the Agreement and Annex 1.

9.2. Restrictions

digiDations will not: (a) sell or share Customer Personal Data, as those terms are defined in the CCPA; (b) retain, use, or disclose Customer Personal Data for any purpose other than the business purposes in Section 9.1, or outside the direct business relationship between digiDations and Licensee; or (c) combine Customer Personal Data with personal information it receives from or on behalf of others, except as the CCPA permits.

9.3. Compliance

digiDations will comply with the obligations that US State Privacy Laws impose on service providers and processors and will provide the same level of privacy protection they require. digiDations will notify Licensee if it determines it can no longer meet those obligations. On notice, Licensee may take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data and may take reasonable steps under Section 10 to confirm that digiDations uses Customer Personal Data consistently with Licensee's obligations.

9.4. Certification

digiDations certifies that it understands and will comply with the restrictions in this Section 9.

10. Audits and Compliance Information

10.1. Compliance Information

On written request, no more than once per year, digiDations will provide its current ISO/IEC 27001 and Cyber Trust mark (Advocate tier) certificates with their scope statements, subject to confidentiality. The parties intend this information to satisfy Licensee's audit rights under Data Protection Laws and Clause 8.9 of the SCCs.

10.2. Further Audits

Licensee may conduct a further audit of digiDations' compliance with this DPA only where: (a) the information in Section 10.1 is reasonably insufficient to demonstrate compliance; (b) a Supervisory Authority or applicable law requires it; or (c) a Personal Data Breach has occurred.

10.3. Audit Conditions

A further audit must:

a. be requested on at least **thirty (30) days**' written notice, or shorter notice where required by a Supervisory Authority or following a Personal Data Breach;
b. follow a scope, timing, and duration agreed in advance;
c. take place no more than once in any **twelve (12)-month** period, except under Section 10.2(b) or (c);
d. be conducted remotely where practicable, during normal business hours, without unreasonable disruption;
e. be performed by Licensee or an independent auditor who is not a digiDations competitor and is bound by confidentiality obligations; and
f. not give access to other customers' data or to information that would compromise the security of digiDations' systems or facilities.

10.4. No Security Testing

An audit does not include penetration testing, vulnerability scanning, or other security testing of digiDations' systems unless digiDations agrees separately in writing.

10.5. Costs and Results

Licensee bears its own audit costs. digiDations may charge reasonable fees for time spent supporting an audit beyond **two (2) business days**, except where the audit reveals a material breach of this DPA by digiDations. Licensee will share the audit report with digiDations and treat it as digiDations Confidential Information.

11. Return and Deletion

11.1. Export and Deletion

On expiry or termination of the Agreement, Licensee may export Customer Data as provided in Section 9.4 of the EULA. digiDations will then delete Customer Personal Data as provided in Section 9.5 of the EULA, unless applicable law requires retention. Any retained data remains subject to this DPA and is processed only for the purpose the law requires.

11.2. Backups

Residual copies of Customer Personal Data in backups are deleted in the ordinary course of backup rotation, and in any event within **ninety (90) days** after deletion from production systems. Until deleted, they remain protected under this DPA and are not actively processed.

11.3. Certification

On written request, digiDations will certify deletion in writing. For the SCCs, this Section 11 satisfies Clauses 8.5 and 16(d), and certification is given only on request.

12. Customer-Hosted Software and AI Features

12.1. Customer-Hosted Software

Licensee controls the environment in which Customer-Hosted Software runs, and digiDations does not process Customer Personal Data held there except: (a) support materials Licensee chooses to share; (b) license activation requests and update checks, which may include the IP address of the requesting system; (c) remote support sessions Licensee grants; and (d) AI-enabled features under Section 12.2. This DPA applies to that limited processing.

12.2. AI-Enabled Features

When AI-enabled features, including those of TARA AI, use the LLM service made available through digiDations, in SaaS or Customer-Hosted deployments, prompts and context are sent through digiDations' AWS account to AI models in Amazon Bedrock in the AWS Asia Pacific (Singapore) region. Prompts may include findings, asset and configuration data, and any Personal Data they contain. AWS acts as a Subprocessor, and the providers of the models do not receive Customer Personal Data. Under AWS's terms for Amazon Bedrock, prompts and outputs are not used to train models, and digiDations does not use Customer Personal Data to train models, as provided in Section 6.4 of the EULA.

12.3. Customer-Selected LLM

For customer-hosted deployments of TARA AI, ATLAS, and APOLLO, Licensee may configure a supported Customer-selected LLM instead of the LLM service made available through digiDations. For features using a Customer-selected LLM, the processing described in Section 12.2 does not occur, and Licensee's arrangements with its LLM provider govern that processing. SaaS deployments use the LLM service made available through digiDations. ATLAS can be used without invoking its LLM-enabled features.

13. Liability, Term and General

13.1. Liability

Each party's liability arising out of or in connection with this DPA, including the SCCs to the extent permitted by law, is subject to the exclusions and limitations in Section 8.4 of the EULA, including the Enhanced Cap where Section 8.4 of the EULA applies it. Nothing in this DPA limits the rights of Data Subjects under the SCCs or any liability that cannot be limited by law.

13.2. Term

This DPA applies for as long as digiDations processes Customer Personal Data under the Agreement and survives termination until that data is deleted under Section 11.

13.3. Changes

digiDations may update this DPA to reflect changes in Data Protection Laws or recognized transfer mechanisms, or to add protections, provided the update does not materially reduce the protection of Customer Personal Data. Subprocessor changes follow Section 5. Any other material change adverse to Licensee requires Licensee's acceptance under Section 10.5 of the EULA.

13.4. Affiliates

Licensee's Affiliates authorized to use the Products under Section 2.2 of the EULA benefit from this DPA. Licensee exercises rights under this DPA on their behalf and remains responsible for their instructions.

13.5. Governing Law

This DPA is governed by the law governing the Agreement, except where Data Protection Laws or the SCCs require otherwise.

13.6. Severability

If a provision of this DPA is invalid or unenforceable, the rest of this DPA remains in effect.

Optional execution. This DPA is effective on Licensee's acceptance of the Agreement and does not require signature. Where Licensee requests a countersigned copy, the parties may sign below.

digiDations Pte. Ltd.

Signature: _____

Name: _____ Title: _____ Date: _____

Licensee: _____

Signature: _____

Name: _____ Title: _____ Date: _____

ANNEX 1: DESCRIPTION OF PROCESSING

A. Parties

Role	Party	Contact	Activity
Data exporter (Controller or Processor)	Licensee and its authorized Affiliates, as named in the Order	Licensee's notice contact in the Order	Use of the Products under the Agreement
Data importer (Processor)	digiDations Pte. Ltd., 20 Anson Road, #06-16, Singapore 079912	Data protection officer, privacy@digidations.com	Provision of the Products under the Agreement

Signature and date: Each party is deemed to have signed this Annex 1, including for the purposes of the Standard Contractual Clauses and UK Addendum, on the date Licensee accepts the Agreement.

B. Description of transfer and processing

Item	Description
Categories of Data Subjects	Authorized Users; Licensee's employees, contractors, customers, and other individuals whose Personal Data is present in systems, applications, directories, files, or cloud services within the scope of testing; individuals named in support communications
Categories of Personal Data	Authorized User account data (name, business email, role, log-in and activity logs, IP address); identifiers found in assessed environments (usernames, email addresses, group memberships, hostnames and device identifiers linked to individuals, IP and MAC addresses); credential material discovered during testing (password hashes, cleartext passwords, tokens, keys); screenshots and file excerpts captured as evidence; AI prompts and outputs containing any of the above; support communications
Sensitive data	Not intended. Special categories of Personal Data may be collected incidentally where present in accessed systems or files. Safeguards: restricted access, encryption, Licensee-controlled scope and evidence settings, and retention as described in the Retention row below
Frequency of transfer	Continuous for the subscription term
Nature of processing	Collection through scanning, testing, and agents; storage; analysis and correlation; reporting; AI inference; support; deletion
Purpose	Providing the Products, including exposure discovery, validation, prioritization, and remediation reporting; support; maintaining the security and operation of the Products
Retention	The subscription term, then export and deletion under Sections 9.4 and 9.5 of the EULA and Section 11 of this DPA
Transfers to Subprocessors	As listed in Annex 3, for the purposes stated there

C. Competent supervisory authority

For EEA transfers, the supervisory authority determined under Clause 13(a) of the SCCs: the authority of the Member State where Licensee is established or, where Licensee has appointed a representative under Article 27 of the EU GDPR, the authority of that representative's Member State. Where Licensee is not established in the EEA and is not required to appoint a

representative under Article 27(2) of the EU GDPR, the supervisory authority of a Member State in which the Data Subjects whose Personal Data is transferred are located. For UK transfers, the UK Information Commissioner. For Swiss transfers, the Swiss Federal Data Protection and Information Commissioner.

ANNEX 2: TECHNICAL AND ORGANIZATIONAL MEASURES

digiDations operates an information security management system certified to ISO/IEC 27001 and holds Cyber Trust mark certification (Advocate tier), each within the scope stated in its certificate. The measures below apply to Customer Personal Data under digiDations' control.

Area	Measures
Governance	Written information security policies reviewed at least annually; designated security and data protection responsibilities; risk assessments; supplier security reviews before engaging Subprocessors
Personnel	Confidentiality agreements; security and data protection training on joining and periodically; prompt removal of access on departure
Access control	Role-based access on a least-privilege and need-to-know basis; multi-factor authentication for administrative and remote access; periodic access reviews; logging of privileged actions
Encryption	Encryption of Customer Data in transit over public networks using current TLS; encryption of Customer Data at rest, including backups
Credential handling	Credential material discovered during testing is encrypted at rest, masked in the user interface by default, and accessible only to Authorized Users with appropriate roles
Logical separation	Logical separation of each Licensee's Customer Data in the SaaS environment; network segmentation between production, corporate, and development environments
Physical security	SaaS infrastructure housed in a third-party colocation facility in Singapore with controlled entry, visitor logging, CCTV, and environmental protections; the facility provider has no logical access to Customer Data
Monitoring and logging	Security event logging and monitoring of production systems; protection of logs against tampering; alerting on suspicious activity
Vulnerability management	Regular vulnerability scanning and patching of production systems based on severity; periodic penetration testing
Secure development	Secure development practices; code review; code signing of Customer-Hosted Software and updates; protection of build, update, and distribution infrastructure
Incident response	Documented incident response procedure; breach notification under Section 7 of this DPA; post-incident review
Business continuity	Regular backups; documented continuity and recovery procedures tested periodically
AI features	AI inference for the LLM service made available through digiDations runs through Amazon Bedrock in the AWS Singapore region; no use of Customer Data to train models; access to AI services restricted to digiDations' accounts
Deletion	Deletion of Customer Data under Section 11 of this DPA; secure disposal of storage media

ANNEX 3: AUTHORIZED SUBPROCESSORS

These Subprocessors are authorized at the date of this DPA. The current list is at https://www.digidations.com/legal/subprocessors.

Subprocessor	Purpose	Customer Personal Data processed	Location

Amazon Web Services (Amazon Web Services Singapore Private Limited)	AI model inference via Amazon Bedrock for the LLM service made available through digiDations, in SaaS and Customer-Hosted deployments	AI prompts and outputs, which may include findings, asset and configuration data and Personal Data in them	Singapore (ap-southeast-1)
Microsoft 365, including Teams (Microsoft Regional Sales Pte. Ltd.)	Business email, documents, collaboration, customer communications, and support	Personal Data in support communications and materials Licensee chooses to share	Microsoft's Asia Pacific geography (data centers in Australia, Hong Kong SAR, Japan, Malaysia, Singapore, and South Korea)