DIGIDATIONS PRIVACY POLICY

Effective date: December 1, 2026

1. Scope and Responsibilities

This Privacy Policy explains how digiDations Pte. Ltd., a company incorporated in Singapore ("digiDations"), handles personal data in connection with its websites, business communications, and ATLAS, APOLLO, ORION, HELIOS, and TARA AI, including their modules, management portals, software components, hosted services, and AI-enabled features (collectively, the "Products"). It covers both customer-hosted software and software as a service ("SaaS"). digiDations handles Personal Data in accordance with Singapore's Personal Data Protection Act 2012 ("PDPA") and other data protection laws applicable to the relevant activity.

"Personal Data" means information about an individual who can be identified from that information or together with other information available or likely to be available to digiDations, subject to applicable law. A "Customer" is an individual or organization subscribing to or evaluating a Product, including the Licensee under the applicable End User License Agreement ("EULA"). "Customer Data", "Confidential Information", and "Authorized User" have the meanings given in the EULA or other applicable agreement.

digiDations determines the purposes of processing information used for its own account administration, business relationships, and operational responsibilities. Where it processes Personal Data solely on a Customer's behalf under a written agreement, it acts as a data intermediary or equivalent processor on the terms of the Data Processing Addendum at https://www.digidations.com/legal/dpa or other applicable agreement. The Customer determines the purposes of that processing and is responsible for the applicable notices, permissions, and lawful instructions; digiDations remains responsible for its own legal and contractual obligations.

2. Information Collected and Its Sources

The information handled depends on the Product, deployment, configuration, and interaction with digiDations. Relevant categories include:

a. Business and Account Information: names, business contact details, organization and role, account identifiers, permissions, and correspondence supplied for inquiries, demonstrations, evaluations, account administration, or support.
b. Purchase and Subscription Information: subscribed Products, license information, entitlements, purchase and renewal records, and relevant billing or payment records received directly or through an authorized reseller or distributor. Information held by a seller or payment provider is also subject to that organization's applicable privacy practices.
c. Technical and Support Information: connection and authentication information needed for online interactions, such as IP addresses and relevant browser or device details, and diagnostic logs, screenshots, system details, or other materials supplied or made accessible for authorized support. For customer-hosted software, the only information sent to digiDations automatically is the activation, license retrieval, and update checks described in Section 4.1. Diagnostic logs, agent data, and security findings remain in the Customer's environment and reach digiDations only if the Customer shares them for support or uses digiDations' LLM service as described in Section 4.2. With the Customer's authorization,

digiDations may provide support through a remote session, such as screen sharing through Microsoft Teams or another tool the Customer chooses, in which digiDations personnel may view and, where the Customer permits, operate the Customer's systems. Information visible during a session is used only to provide the requested support. Sessions are not recorded unless the Customer agrees in advance.

d. Customer Content: information submitted, collected from authorized targets, or generated through configured Product functionality, including security findings, reports, prompts, and outputs. It may contain Personal Data depending on the Customer's systems and use. "Customer Data" and customer-specific outputs remain subject to the applicable agreement.

Information may come from individuals, Customer administrators and Authorized Users, authorized channel partners, or service providers supporting the relevant transaction or functionality. If a Customer enables a third-party sign-in or integration, digiDations receives the information authorized through that connection. Publicly available business information is used only where relevant and lawfully permitted.

digiDations seeks information relevant to the stated purpose. Customers and users should avoid submitting unnecessary identification documents, sensitive personal information, or unrelated personal content. Business contact information may receive different treatment under Singapore law; this Policy also explains digiDations' handling of that information.

3. Purposes and Grounds for Processing

digiDations handles relevant information to respond to inquiries; administer accounts, purchases, and subscriptions; validate licenses; provide configured Product functionality; investigate support requests; maintain service security and integrity; prevent unauthorized use and fraud; communicate operational changes; and meet legal, recordkeeping, and dispute-resolution requirements.

Customer Data processed on a Customer's behalf is used within the applicable agreement and lawful instructions to provide, secure, support, and maintain the subscribed Products. digiDations does not use Customer Data for marketing or to train models.

Where consent is required, digiDations obtains it. Otherwise, digiDations processes Personal Data only where applicable law permits processing without consent, such as to perform a contract, comply with legal obligations, or pursue legitimate interests subject to the required assessment and safeguards. A Customer is responsible for the legal basis of processing it directs.

Before using Personal Data for an additional purpose, digiDations provides any required notice and obtains consent or establishes another permitted ground. Any additional use of Customer Data must also remain within the applicable Customer agreement.

4. Product Deployment and AI Processing

4.1. License Activation and Hosting

To activate customer-hosted software, the Customer provides the license file supplied by digiDations during onboarding. The software sends a unique key from that file to digiDations' license activation service, which confirms the license and records the activation. When a subscription is renewed or extended, digiDations updates the license in its licensing system, and the software retrieves and installs the updated license automatically.

Customer-hosted software also checks digiDations' update service for software updates and new attack or threat content. These checks send the installed product version and an identifier for the installation.

Activation requests, license retrieval, and update checks also carry standard connection information, such as the IP address and time of the request. Customers can turn off these automatic connections in the product settings, for example in air-gapped deployments. In that case, license renewal and updates stop being retrieved automatically, and the Customer installs renewed licenses from a license file supplied by digiDations and installs updates manually. No other information about the Customer's environment is sent automatically.

For customer-hosted software, the Customer controls its hosting environment and configuration. Installation does not, by itself, grant digiDations access to the environment or its contents. Separate transmissions may occur through selected AI features, connected services, or authorized support. For SaaS, digiDations processes information needed to operate the hosted Product in digiDations-operated infrastructure in Singapore, within the applicable agreement.

4.2. Choice of LLM and Processing of Prompts

Some Products use an AI or large language model ("LLM") connection. TARA AI and APOLLO require an LLM connection for core functionality. ATLAS offers LLM-enabled features as an optional enhancement, and ATLAS can be used without invoking them. For customer-hosted deployments of these Products, a Customer may use a supported Customer-selected LLM instead of the LLM service made available through digiDations. The Customer-selected LLM may operate on premises or through a cloud provider. SaaS deployments use the LLM service made available through digiDations.

Where digiDations' LLM service is used, prompts and outputs are processed through Amazon Bedrock in the AWS Singapore region, as listed at https://www.digidations.com/legal/subprocessors. Prompts and outputs may contain Personal Data included in the submitted materials. The providers of the underlying models do not receive this data, and prompts and outputs are not used by digiDations, AWS, or the model providers to train or fine-tune models. digiDations may change the models it uses. Any change to the provider that processes this data is made in accordance with the notice commitments in the applicable agreement.

For a Customer-selected LLM, the configured integration determines the data flow. The Customer establishes the necessary permissions and arrangements with its provider. This choice does not itself authorize digiDations to access that LLM environment, and does not eliminate processing otherwise necessary to host, operate, secure, or support the Product.

4.3. Model Training and Service Improvement

digiDations does not use Customer Data, including prompts and outputs, to train or fine-tune models, whether general-purpose, specialized, or customer-specific, and does not permit its AI providers to do so.

digiDations does not collect analytics about how individual users use the Products. Technical and operational information generated in operating the Products, such as license activation and update records and, for SaaS, system, performance, and security logs, is used only to operate, secure, support, and maintain the Products and to meet legal requirements. digiDations' published threat research is based on threat intelligence it collects through its own sources and does not include Customer Data.

digiDations does not itself make decisions about individuals that produce legal or similarly significant effects based solely on automated processing. AI-enabled features either carry out specific tasks configured by the Customer or propose actions for review. AI-generated actions that could disrupt or change a Customer's production systems, such as attack simulation against production assets or configuration changes, require approval by an Authorized User at the time the action is proposed, unless the Customer configures otherwise where the Product allows. Product outputs, including AI-generated findings, are provided to the Customer, which determines any resulting actions.

5. Cookies and Third-Party Services

digiDations' website uses cookies and similar technologies that are necessary for site functions and security, analytics tools (Google Analytics, HubSpot, and Cloudflare Web Analytics) to understand how visitors use the website, HubSpot for contact forms and related website interactions, and the LinkedIn Insight Tag to measure the effectiveness of digiDations' advertising on LinkedIn and to show relevant advertising to website visitors on LinkedIn. Non-essential cookies are used only with the visitor's consent where required by law, and visitors can change their choices at any time through the cookie settings on the website. Information submitted through contact and inquiry forms is stored in digiDations' customer relationship management system. digiDations does not use session-recording tools. Product portals use only cookies necessary for authentication, session management, and security. Details of the cookies used and how to manage them are in the Cookie Policy at https://www.digidations.com/legal/cookies.

Websites and Products may link to, or support connections with, services selected by the Customer. Those providers' notices govern their independent processing. This does not relieve digiDations of responsibility for providers processing information on its behalf.

6. Information Sharing

digiDations discloses information only as relevant to the stated purpose, the applicable agreement, and law. Recipients may include:

a. Authorized Personnel and Service Providers: personnel with a need to know and providers of website hosting, IT operations, licensing, support, AI processing, communications, customer relationship management, website analytics, advertising measurement, and transaction services. Providers processing Customer Data on digiDations' behalf are subject to appropriate written confidentiality, security, processing, and deletion obligations. digiDations remains responsible for their performance of its contractual obligations. A current list of Subprocessors that process Customer Data is available at https://www.digidations.com/legal/subprocessors.
b. Resellers, Distributors, and Business Partners: relevant contact, transaction, subscription, and support information needed to fulfill the Customer's purchase or requested services. A channel relationship does not, by itself, authorize access to Product content, security findings, prompts, or outputs.
c. Professional Advisers and Authorities: advisers assisting with legal, audit, or other professional responsibilities, and competent authorities or other recipients where disclosure is legally required or permitted to investigate unlawful activity or protect legal rights, subject to applicable confidentiality and processing restrictions.
d. Business Successors: recipients involved in a proposed or completed merger, reorganization, financing, or transfer of the relevant business, subject to lawful disclosure, appropriate confidentiality safeguards, and the applicable Customer agreement.

Customer Data is not provided to advertisers or data brokers for their independent commercial use. Other disclosures require the relevant permission or another lawful ground and must remain within applicable contractual restrictions.

7. International Processing and Storage

Information may be stored or processed in Singapore and other countries where digiDations or the relevant providers operate. SaaS Customer Data is hosted in Singapore, and prompts sent to digiDations' LLM service are processed in Singapore. Business contact, website, and analytics information may be processed by service providers in other countries, including the United States. Support communications and materials shared through Microsoft 365 are stored in Microsoft's Asia Pacific geography. A Customer-selected cloud LLM may involve separate transfers arranged by the Customer.

For transfers under digiDations' responsibility, digiDations applies safeguards required by applicable law, including comparable protection for Personal Data transferred from Singapore where required. Depending on the applicable law and arrangement, safeguards may include enforceable contractual obligations or another legally recognized transfer mechanism.

An agreed hosting-region or data-residency restriction remains binding and cannot be expanded by this Policy. Customers may contact digiDations for information about the safeguards relevant to their processing. Additional legally required transfer arrangements are established where applicable.

8. Security and Data Breaches

digiDations applies reasonable technical, organizational, and physical safeguards appropriate to the information and processing risks. These address authorized access, authentication, protection of information in storage and transmission, confidentiality, secure handling and disposal, and incident response. Measures are reviewed as risks and services change. No system or transmission method can guarantee absolute security.

Customers remain responsible for the security of their own environments, user permissions, credentials, and Customer-controlled integrations. Suspected account compromise or inappropriate disclosure should be reported promptly through the support channel or privacy contact below.

digiDations assesses information-security incidents and makes notifications to affected Customers, individuals, and regulators as required by applicable law and its agreements. Under the standard EULA, digiDations notifies the Customer without undue delay, and in any event within **seventy-two (72) hours**, after becoming aware of unauthorized access to, disclosure of, or loss of Customer Data under its control. Information may be provided in stages as an investigation progresses.

9. Retention and Deletion

Personal Data is retained only while reasonably necessary for the relevant service, transaction, security, or other stated purpose, or for applicable legal or business requirements. Relevant factors include the subscription and support period, recordkeeping duties, disputes, and lawful preservation requests. When retention is no longer justified, information is securely deleted or irreversibly anonymized, subject to applicable law.

Customer Data export and deletion follow the applicable agreement. Under the standard EULA, SaaS Customers may request standard export during the subscription and for **thirty (30) days** after it ends. Customer Data is then deleted or irreversibly anonymized within **ninety (90) days** after the export period, unless another period is agreed or retention is legally required. Customer-hosted support data is deleted within **ninety (90) days** after it is no longer needed for its authorized support purpose, subject to the same exceptions.

Residual copies of Customer Data in backups are deleted through the backup rotation cycle, and in any event within **ninety (90) days** after deletion from production systems. Until deleted, they remain protected and isolated from ordinary use, and applicable deletion is reapplied if they are restored. Legally retained data is restricted to the retention purpose. Anonymized information may be retained only where individuals and Customers cannot reasonably be identified, and a Customer's Confidential Information is not disclosed. Different agreed arrangements prevail where applicable.

10. Privacy Choices and Individual Rights

10.1. Requests and Consent Withdrawal

Subject to applicable law and its exceptions, individuals may request access to their Personal Data and information about its use or disclosure, correction of inaccurate or incomplete information, and withdrawal of consent on reasonable notice. Depending on the applicable law, additional rights may include deletion, restriction, objection, or portability. These rights apply to the extent provided by the relevant law; they are not unconditional rights to alter or delete all Product records.

Requests may be sent to the privacy contact below. digiDations verifies identity and authority using information proportionate to the request and explains any applicable refusal or limitation. Responses are provided within the applicable legal timeframe. For Singapore access or correction requests that cannot be completed within **thirty (30) days**, digiDations provides written notice within that period of when it expects to respond. Reasonable access fees are charged only where law permits and after advance notice.

Consent withdrawal does not affect processing already lawfully carried out or processing permitted without consent. digiDations explains material consequences, including where requested functionality cannot continue without the relevant processing. Where Customer-controlled data is involved, individuals should contact the Customer first; digiDations refers or assists with requests as appropriate without independently overriding lawful Customer instructions.

10.2. Communications and Complaints

Individuals may decline optional promotional communications through the provided unsubscribe method or the privacy contact. Marketing, including messages to Singapore telephone numbers, is subject to applicable consent, unsubscribe, and Do Not Call requirements. EULA acceptance does not constitute optional marketing consent. Necessary account, security, support, and service notices may continue.

Privacy concerns may be raised with digiDations' Data Protection Officer. Individuals may also complain to Singapore's Personal Data Protection Commission or another competent supervisory authority where applicable. digiDations does not penalize individuals for exercising legally protected privacy rights.

11. Children's Information

The websites and Products are intended for business use and are not directed to children. digiDations does not knowingly solicit Personal Data directly from children for independent account registration or marketing. A parent or guardian who believes a child has provided such information may contact the Data Protection Officer; digiDations will investigate and remove information where required. Incidental information about children within Customer Data remains subject to the applicable Customer instructions and legal safeguards.

12. Additional Information for Individuals in the EEA, UK, and Switzerland

This section applies where the EU General Data Protection Regulation, the UK GDPR, or the Swiss Federal Act on Data Protection applies to digiDations' handling of Personal Data. For Personal Data that digiDations handles for its own purposes as described in this Policy, digiDations Pte. Ltd. is the controller. digiDations relies on the following legal bases:

a. Contract: to administer accounts, purchases, and subscriptions, validate licenses, provide the Products, and provide support.
b. Legitimate interests: to respond to business inquiries, maintain the security and integrity of the websites and Products, prevent fraud and misuse, and communicate with business contacts, where those interests are not overridden by the individual's rights.
c. Legal obligation: to meet recordkeeping, tax, regulatory, and other legal requirements.
d. Consent: for non-essential cookies and for marketing where consent is required. Consent may be withdrawn at any time.

Individuals may request access to, correction, deletion, restriction of processing, and portability of their Personal Data, and may object to processing based on legitimate interests, including at any time to direct marketing. Requests may be sent to the privacy contact below.

Where Personal Data is transferred from the EEA, the UK, or Switzerland to Singapore or another country without an adequacy decision, digiDations uses the European Commission's Standard Contractual Clauses, the UK International Data Transfer Addendum, or another recognized transfer mechanism where required. Individuals may request information about these safeguards from the privacy contact below.

Individuals may also lodge a complaint with the data protection supervisory authority where they live or work, or where an alleged infringement occurred.

13. Changes to This Policy

digiDations may update this Policy to reflect changes in its practices, Products, or legal requirements. The updated version will identify its revision date. Material changes will be communicated through an appropriate channel, such as the website, Product, or Customer contact, with additional notice or consent where required. An update does not amend an existing Customer agreement or retrospectively authorize an incompatible use of Personal Data.

14. Privacy Contact

Questions, requests, and complaints concerning this Policy or the handling of Personal Data may be directed to:

Data Protection Officer
digiDations Pte. Ltd.
20 Anson Road, #06-16
Singapore 079912
Email: privacy@digidations.com

A request should describe the relevant interaction, account or Customer where applicable, and the assistance sought. Unnecessary sensitive information should not be included. digiDations will request additional verification through an appropriate channel if needed.