Privacy Policy

Last updated: 2 July 2026

Your privacy is important to us.

At, UDD Technologies Pte. Ltd. (collectively referred to herein as “UDD Technologies” or “we” or “our”), we value your data privacy and are committed to protecting your personal data. This Privacy Policy ("Policy") describes how UDD Technologies collects, uses, discloses, transfers, stores, and protects personal data and other information in connection with:

- Your access to and use of our corporate website at www.uddtech.com ("Website");
- Your access to and use of the AthenaSpace, a unified platform for workplace management, asset intelligence, and digital signage at www.athenaspace.app ("Platform");
- Any related services, products, communications, and support activities we provide (collectively, the "Services").

This privacy policy applies to you when:

- visit, interact with or use our Site; visit our social media pages; submit a job application; receive online advertisements or communications from us, including emails, phone calls and texts; or register for, attend and/or otherwise take part in our events, tutorials or webinars (we collectively refer to all of these activities as our "Marketing Activities");
- are Administrators, authorised users, and employees of our B2B customers ("Customer Users") who access the Platform under a subscription agreement; and
- End users whose data is processed by the Platform at the direction of our customers ("End Users") (herein customer users and end users collectively referred to as "Service Users") (we collectively refer these activities as the "**Services**" in this Policy).

Roles and Responsibilities

UDD Technologies operates in the following capacities, depending on context:

Context	UDD Technologies' Role	Applicable Obligations
Website data and marketing communications	Data Controller	PDPA (Singapore), GDPR (where applicable)
Account registration and billing data for SaaS customers	Data Controller	PDPA (Singapore), GDPR (where applicable)
Customer content and End User data processed through the Platform	Data Processor	Governed by Data Processing Agreement with Customer
Aggregated, de-identified analytics derived from Platform usage	Data Controller	PDPA (Singapore)

Where UDD Technologies acts as a Data Processor, the Customer is the Data Controller and determines the purposes and means of processing. Our obligations as a processor are governed by the applicable Data Processing Agreement ("DPA") entered with each Customer. This Policy does not override the terms of any DPA.

Governing Legal Framework

This Policy has been drafted to comply with, and should be read in conjunction with, the following legal frameworks:

- **Personal Data Protection Act 2012 (Singapore) ("PDPA"):** As the primary data protection law applicable to our operations as a Singapore-incorporated entity.
- **General Data Protection Regulation (EU) 2016/679 ("GDPR"):** To the extent we process personal data of individuals located in the European Economic Area ("EEA") or the United Kingdom.
- **SOC 2 Trust Services Criteria:** Our security and privacy practices are being developed, assessed and improved with reference to the AICPA Trust Services Criteria applicable to security, availability, confidentiality and/or privacy, as relevant to the scope of our Services.

This Privacy Policy will be continuously assessed against new technologies, business practices and our customers' needs and legal developments, and may be revised accordingly.

This Policy does not apply to any third-party websites, services or applications, even if they are accessible through or are necessary for the use of our Services.

When you access our platform or use our Services or engage with our Marketing Activities, you acknowledge that you have read this Policy and understand its content.

Your use of our platform, Services and interaction through our Marketing Activities, including any dispute over privacy is subject to this Privacy Policy and the terms of service.

Table of Contents

1. What Information do we collect?

The Personal Data we collect depends on the context of your interactions with UDD Technologies and the choices you make (including your privacy and browser settings), the Services you use, your location and applicable law, but can include the following:

1.1 Personal Data You Provide Directly

a. Website Visitors and Prospective Customers

- **Contact and Inquiry Data:** Name, business email address, job title, company name, country, and telephone number provided through contact forms, demo requests, newsletter sign-ups, or event registrations.
- **Marketing Preferences:** Communication preferences you indicate when subscribing to our marketing communications.
- **Correspondence:** Records of communications you initiate with us via email, online chat, or support portals.
- **Applicant information (Employment and Education information):** If you apply for a job with UDD Technologies (such as your resume, desired pay, education and work history, whether you are over the age of 18, and visa status).

b. SaaS Customer Administrators and Users

- **Account Registration Data (Customer records):** Full name, work email address, job title, department, organisation name, and account credentials (hashed passwords) provided during account creation.
- **Billing and Contractual Data:** Company name, registered address, billing address, tax identification numbers, and payment method details (processed via our authorised payment processors; we do not store full card numbers).
- **Support and Communications Data:** Information you provide when submitting support tickets, engaging in our customer success team, or participating in product surveys and feedback forms.
- **Onboarding and Configuration Data:** Workspace configuration settings, user directory imports (where applicable), device registration data for digital signage displays, and integration credentials for connected third-party services.

c. End Users (Processed on Behalf of Customers)

The AthenaSpace Platform may process personal data relating to End Users — employees, visitors, or other individuals within a customer's workplace environment. Such data may include:

- Employee identifiers (name, employee ID, email, department) for room or desk booking, visitor management, and content targeting;
- Visitor management data, including name, host employee, check-in/check-out timestamps, and photographic identification (where configured by the Customer);
- Space utilisation and occupancy data derived from sensor integrations or booking interactions;

- Digital signage interaction data (e.g., content engagement, wayfinding queries) where analytics features are enabled by the Customer.

UDD Technologies processes End User data solely on the documented instructions of the Customer (acting as Data Controller) and as further described in the applicable DPA.

1.2 Usage and Technical Data Collected Automatically

When you access our website or Platform, we automatically collect certain technical and behavioural data, including:

- **Log and Access Data:** IP address, browser type and version, operating system, referral URL, pages visited, timestamps of access, and session duration.
- **Device Information:** Device type, screen resolution, hardware model, unique device identifiers (for registered signage displays), and mobile operating system.
- **Platform Usage Data:** Feature usage patterns, content publishing activity, user interaction logs, API request metadata, error logs, and performance telemetry data.
- **Audit and Compliance Records:** System logs, access logs, security logs, consent or acceptance records, administrator activity records, integration permission records, support access records, import/export records, deletion records and other records generated for security, compliance, audit, troubleshooting, incident investigation and service operation purposes.
- **Location Data:** General geographic location derived from IP address (city/country level). Precise location data is only collected from signage devices where location services are enabled by the Customer administrator.
- **Cookies and Similar Technologies:** As described in Section 10 (Cookies and Tracking Technologies) of this Policy.

1.3 Data Received from Third Parties

- **Identity Providers and SSO:** Where Customers configure Single Sign-On ("SSO") via providers such as Microsoft Azure Active Directory, Okta, or Google Workspace, we receive authentication tokens, user profile attributes (name, email, department), and group membership data as defined by the Customer's SSO configuration.
- **Directory Integrations:** Where Customers enable HRIS or Active Directory synchronisation, we receive employee profile data as configured by the Customer administrator.

- **IoT and Sensor Integrations:** Aggregated or anonymised occupancy and environmental data received from connected IoT devices or building management systems configured by the Customer.
- **Business Partners and Resellers:** Contact and account data relating to prospective customers introduced to us by authorised channel partners or resellers.
- **Public Sources:** Publicly available professional information (e.g., LinkedIn profiles) to enrich our understanding of prospective customer organisations, used solely for B2B sales and marketing purposes.

1.4 Data We Do Not Intentionally Collect

We do not intentionally collect the following categories of sensitive personal data through our standard Service operations. Customers and End Users should not submit such data to the Platform except where expressly contemplated by a specific contractual agreement and applicable Data Protection Impact Assessment:

- Government-issued identification numbers (e.g., NRIC, passport numbers), except where a customer has enabled visitor identity verification features;
- Financial account credentials or payment card data (processed only through PCI-DSS-compliant third-party payment processors);
- Health, medical, or biometric data (except anonymised occupancy signals);
- Racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, or data concerning a person's sex life or sexual orientation;
- Personal data of individuals under eighteen (18) years of age (see Section 12 — Children's Data).

2. How we collect Data?

2.1 Data Provided Directly by You

We collect personal data directly from you when you:

- Complete and submit forms on our website (e.g., contact, demo request, event registration);
- Register for or log in to your AthenaSpace platform account;
- Configure the Platform, manage user accounts, or connect third-party integrations;

- Contact our sales, support, or customer success teams via email, telephone, or live chat;
- Participate in surveys, beta programmes, webinars, or other promotional activities;
- Execute a subscription agreement, order form, or other contractual document with us.

2.2 Data Collected Automatically

Automated data collection occurs when you visit our website or access the Platform through mechanisms including:

- Server and application log files maintained by our cloud infrastructure;
- Cookies, web beacons, and similar tracking technologies (see Section 10);
- Software Development Kit (SDK) components embedded within the Platform for performance monitoring and error tracking;
- Device telemetry agents on registered digital signage hardware devices.

2.3 Data Received from Third-Party Systems

- Data may be received from third-party systems integrated with the Platform at the Customer's direction, including:
- Identity and access management systems (e.g., SSO providers, Active Directory);
- Human Resources Information Systems ("HRIS") connected by the Customer;
- Calendar and collaboration platforms (e.g., Microsoft 365, Google Workspace) connected for room booking and scheduling features;
- IoT infrastructure, sensor networks, or building management systems;
- Content delivery platforms and third-party application integrations which are available through the AthenaSpace platform marketplace.

3. Information We Process on Behalf of our Customers

Our Services are intended for use by our business customers. As a result, for much of the Personal Data we process through the Services, we act as a processor or service provider on behalf of our business customers. This means that it is our business customers that control what Personal Data we collect through the Services and how we use it. Where our activities as a processor or service provider are clear and consistent across our customer base, we have described those activities herein in the interests of transparency. However, if you are a Service User, and have privacy related questions or

concerns about the privacy practices of or the choices the relevant business customer has made regarding your information via the Services, you should contact the relevant customer (e.g. your employer) directly or review their privacy notices.

We are not responsible for the privacy or data security practices of our business customers, which may differ from those set forth in this Policy.

4. Purposes of Processing

We process personal data for the following purposes. Where GDPR applies, the corresponding legal basis is indicated in Section 5.

Purpose	Categories of Data	Applies To
Service Delivery — Provision, operation, maintenance, and support of the Platform and Services.	Account data, usage data, configuration data, End User data	Customer Users, End Users
Account Management — Creating and managing user accounts, authenticating users, and enabling access controls.	Account registration data, authentication data	Customer Users
Customer Support — Responding to inquiries, resolving incidents, and providing technical assistance.	Contact data, support correspondence, usage logs	Website visitors, Customer Users
Billing and Contract Administration — Processing payments, issuing invoices, and managing contractual relationships.	Billing data, contractual data	Customer Administrators
Security and Fraud Prevention — Detecting,	Log data, usage data, technical data	All users

Purpose	Categories of Data	Applies To
investigating, and preventing security incidents, fraud, and misuse.		
Product Analytics and Improvement — Analysing aggregated Platform usage to improve features and user experience.	Anonymised/aggregated usage data	Customer Users, End Users (anonymised)
Marketing and Communications — Sending product updates, newsletters, event invitations, and promotional offers (with consent or legitimate interest).	Contact data, marketing preferences	Website visitors, prospective customers
Legal and Regulatory Compliance — Meeting our obligations under applicable laws, including retention, audit, and disclosure requirements.	All categories as required	All users
Research and Development — Developing new product features using de-identified, aggregated datasets.	Anonymised usage and telemetry data	All users (anonymised)

Purpose	Categories of Data	Applies To
Audit, Compliance and Security Evidence – maintaining records required for security monitoring, access control, incident investigation, legal compliance, audit readiness, dispute resolution and certification or assurance processes.	audit logs, access logs, security logs, administrator activity records, support access records, acceptance records, integration records, import/export records and related metadata	Customer Users, End Users, administrators and support personnel.

We may create, use, retain and disclose Aggregated Data and Anonymised Data for analytics, benchmarking, reporting, research, product development, service improvement, security, operational and other legitimate business purposes.

Aggregated Data and Anonymised Data do not identify you, our customers, Customer Users, End Users or any individual. We do not treat such data as personal data where it cannot reasonably be used to identify an individual.

Where we anonymise or aggregate data, we take steps designed to reduce the risk of re-identification, having regard to the nature of the data, the context of processing, the safeguards applied and the information that we have or are likely to have access to.

5. Legal Basis for processing

5.1 Applicability

Where the GDPR applies to processing activities (i.e., where we process personal data of individuals in the EEA or UK), we are required to identify a legal basis for each processing activity. The following legal bases apply:

5.2 Legal Bases

- **Performance of a Contract (Article 6(1)(b) GDPR):** Processing is necessary to perform the SaaS subscription agreement with the Customer, including account management, service delivery, and billing.

- **Compliance with a Legal Obligation (Article 6(1)(c) GDPR):** Processing is necessary to comply with applicable legal requirements, including tax, accounting, security incident notification, and law enforcement obligations.
- **Legitimate Interests (Article 6(1)(f) GDPR):** Where GDPR applies and where we act as an independent controller, we may process personal data where necessary for our legitimate interests, including securing and improving our Services, maintaining service reliability, conducting product analytics, preventing fraud and misuse, responding to customer requests, maintaining audit and compliance records, and conducting B2B marketing, provided such interests are not overridden by the interests, rights or freedoms of the relevant individual. Where we process personal data as a processor on behalf of a customer, the customer is responsible for determining the applicable legal basis for the relevant processing activity. In such cases, we process personal data in accordance with the customer's instructions and applicable contractual terms.
- **Consent (Article 6(1)(a) GDPR):** Where we rely on consent — for example, for optional marketing communications or non-essential cookies — we will request your explicit consent. Consent may be withdrawn at any time without affecting the lawfulness of processing prior to withdrawal.
- **Vital Interests / Public Task:** Applied only in exceptional circumstances not forming part of our standard operations.

5.3 Applicability under the Singapore PDPA

Under the PDPA, we may collect, use, and disclose personal data:

(a) with the consent of the individual, where consent is required;

(b) where deemed consent applies under the PDPA;

(c) without consent where an exception under the PDPA applies, including where applicable for legitimate interests, business improvement, research, evaluative purposes, publicly available data, business asset transactions, investigations or other purposes permitted by law;

(d) where the data constitutes business contact information and is used for business-to-business communications; and

(e) where we process personal data as a data intermediary on behalf of and for the purposes of a customer pursuant to a written contract.

Where we use personal data for analytics, service improvement or research, we will use

Aggregated Data or Anonymised Data where practicable. Where identifiable personal data is used, we will limit such use to what is reasonably necessary and permitted by applicable law, contract or customer instructions.

6. Data Sharing and Disclosure of your information

UDD Technologies does not sell, rent, or trade personal data. We do not use Customer Data or End User personal data for third-party advertising purposes. We do not disclose Customer Data or End User personal data to third parties for their own independent marketing purposes unless the relevant customer or individual has expressly authorised us to do so, or unless such disclosure is otherwise permitted or required by applicable law.

For the avoidance of doubt, our use of Usage Data, Aggregated Data and Anonymised Data for service operation, security, analytics, benchmarking, reporting, research, product development and service improvement is not treated as a sale of personal data.

We may share personal data in the following circumstances:

6.1 Sub-Processors and Service Providers

We engage authorised affiliates, sub-processors, vendors, contractors and third-party service providers to support the delivery, operation, maintenance, security, analytics, improvement and support of our Services. These parties may process personal data only for the purposes for which they are engaged and are subject to appropriate contractual obligations relating to confidentiality, data protection and security.

Our current categories of sub-processors include:

Category	Examples	Purpose
Cloud Infrastructure	Microsoft Azure	Platform hosting, compute, storage, networking
Monitoring & Observability	Microsoft Azure, Aikido, Atlassian	Performance monitoring, logging, alerting
Customer Support	Atlassian, Salesforce	Support ticket management
Marketing Automation	Salesforce, Storylane	Email communications, CRM

Category	Examples	Purpose
Analytics	Salesforce, Oracle	Product usage analytics (anonymised/aggregated)
Payment Processing	Oracle NetSuite, Salesforce	Billing and payment processing
Video Conferencing / Collaboration	Microsoft Teams, Slack	Customer onboarding and support calls
Identity / SSO	Microsoft Azure, Microsoft Entra ID	Authentication services

An up-to-date list of our sub-processors is available upon written request to privacy@udd.tech.

6.2 Customer Disclosure

Where UDD Technologies acts as a Data Processor, we disclose processed data to the relevant Customer (as Data Controller) in accordance with the applicable DPA and the Customer's documented instructions. Customers are responsible for the lawful use and further disclosure of such data within their organisations.

6.3 Business Partners and Resellers

Where you are introduced to us through an authorised reseller or channel partner, we may share relevant account and support data with that partner to facilitate service delivery, consistent with the terms of our partner agreements.

6.4 Legal Obligations and Law Enforcement

We may disclose personal data where required to do so by applicable law, regulation, court order, or at the request of a regulatory authority, including:

7. Compliance with mandatory disclosure obligations under Singapore law or other applicable jurisdictions;
8. Protection of the rights, property, or safety of UDD Technologies, our customers, or others;
9. Detection, investigation, or prevention of illegal activity, fraud, or security incidents.

Where permitted by law, we will notify the relevant Customer or individual prior to or promptly following such disclosure.

6.5 Corporate Transactions

In the event of a merger, acquisition, restructuring, sale of assets, or insolvency proceedings involving UDD Technologies, personal data may be disclosed to prospective or actual acquirers and their advisors as part of due diligence, subject to appropriate confidentiality obligations. We will notify affected parties of any such change in ownership or control as required by applicable law.

6.6 Consent-Based Sharing

We may share personal data with other third parties where you have provided express prior consent for such sharing.

7. International Data Transfers

7.1 Primary Processing Location

UDD Technologies is headquartered in Singapore. Our primary cloud infrastructure is hosted on Microsoft Azure, with data centres located in Singapore and other Southeast Asian countries. Personal data relating to Platform users is primarily processed and stored within the Singapore Azure region.

7.2 Cross-Border Transfers

While delivering our Services, personal data may be transferred to, accessed from, or stored in countries other than the country in which it was collected, including other jurisdictions in Southeast Asia, the United States, the EEA, and Australia. Such transfers may occur in connection with:

- Our sub-processors and service providers operate in multiple jurisdictions (see Section 6.1);
- Customer administrators and end users accessing the Platform from multiple countries;
- Support and customer success teams operating across our office locations.

7.3 Safeguards for International Transfers

We implement the following safeguards to protect personal data transferred internationally:

- **Singapore PDPA — Section 26 Obligations:** Where personal data is transferred outside Singapore, we ensure the recipient provides a standard of protection comparable to the PDPA, through contractual data transfer arrangements,

binding corporate rules, or reliance on the PDPC's approved adequacy framework.

- **GDPR — Standard Contractual Clauses (SCCs):** For transfers from the EEA or UK, we use the European Commission's approved Standard Contractual Clauses (2021) or the UK International Data Transfer Addendum (IDTA), as applicable.
- **Adequacy Decisions:** Where the European Commission or UK ICO has issued an adequacy decision in respect of the destination country, we rely on such decision.
- **Contractual Protections:** All sub-processor agreements include data transfer provisions consistent with applicable law.

7.4 Data Residency

Customers with specific data residency requirements (e.g., requirement to process data exclusively within Singapore or another jurisdiction) may request data residency configurations as part of their subscription agreement. Please contact our team to discuss data residency options.

8. Data Retention

8.1 Retention Principles

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, to comply with our legal and regulatory obligations, to resolve disputes, and to enforce our agreements. Retention periods are determined with regard to the following criteria:

- The nature and sensitivity of the personal data;
- The purposes for which the data is processed and whether those purposes can be achieved through other means;
- Legal, regulatory, and contractual requirements applicable to specific data categories;
- The period necessary to establish, exercise, or defend legal claims.

We may retain Usage Data, Aggregated Data, Anonymised Data, audit logs, security logs and compliance records for longer periods where reasonably necessary for analytics, service improvement, security, compliance, audit, dispute resolution, legal or regulatory purposes, subject to applicable law and our internal retention policies. Where such retained data identifies an individual, we will retain it only for as long as reasonably necessary for the relevant purpose or as otherwise permitted or required by law.

8.2 Deletion and Anonymisation

Upon expiry of the applicable retention period, personal data is securely deleted, anonymised, or de-identified using industry-standard methods, such that re-identification is not reasonably possible. Anonymised and aggregated data may be retained indefinitely for analytical and reporting purposes.

8.3 Customer-Initiated Deletion

Customers may request deletion of their account data and all associated Customer Content at any time by contacting privacy@udd.tech or through the account management console, subject to any applicable minimum retention obligations.

9. Security Measures

UDD Technologies takes the security of personal data seriously. We implement and maintain a comprehensive information security programme designed to protect the confidentiality, integrity, and availability of personal data processed through our Services. Our information security and privacy programme is intended to support our compliance, assurance and certification readiness efforts, including readiness for SOC 2 assessment where applicable to the scope of our Services.

We have security measures in place to protect against the loss, misuse, and alteration of the information under our control. These security measures include a firewall to prevent unauthorized access to our systems and encryption of all password information. Although we will exercise reasonable care in providing secure transmission of information between your computer and our servers, we cannot ensure or warrant the security of any information transmitted to us over the Internet and we accept no liability for any unintentional disclosure.

We maintain security monitoring, access control and audit evidence processes designed to protect the confidentiality, integrity and availability of personal data and Customer Data processed through the Platform.

These measures may include, as appropriate:

(a) role-based access controls and user permission management;

(b) authentication controls, including password controls and multi-factor authentication where enabled or required;

(c) access logging and monitoring of administrator, support, system and user activity;

(d) audit logs recording relevant security, access, configuration, support, import, export,

deletion and system events;

(e) periodic access reviews and access revocation processes;

(f) controls for support access to customer environments, including access limitation, purpose-based access and access logging where practicable;

(g) vulnerability management, patch management, backup and recovery controls;

(h) incident detection, escalation, investigation and response processes; and

(i) retention of security, audit and compliance evidence to support legal, regulatory, contractual, certification and assurance requirements.

Access to personal data and Customer Data is limited to authorised personnel, service providers and sub-processors who require such access for legitimate business, operational, security, support, compliance or legal purposes and who are subject to appropriate confidentiality and security obligations.

Employee Access

Our corporate values, ethical standards, policies and practices are committed to the protection of customer information. In general, our business practices limit employee access to confidential information, and limit the use and disclosure of such information to authorized persons, processes and transactions.

10. Cookie and other tracking technologies

We may, and we may allow third party service providers to, use cookies or other tracking technologies to automatically collect information from your computer or mobile device about your browsing activities over time and across different websites following your use of the Site, your interaction with our Marketing Activities as well as in connection with the Services.

We may use cookies, web beacons, pixels, software development kits, local storage, log files and similar technologies in connection with our Website and Platform.

These technologies may be used for the following purposes:

(a) Strictly Necessary Purposes: to enable core Website and Platform functionality, including authentication, session management, account access, security, fraud prevention, load balancing, user preferences and service availability;

(b) Performance and Diagnostic Purposes: to monitor service performance, detect errors, diagnose technical issues, measure uptime, understand system reliability and improve the stability of the Website and Platform;

(c) Product Analytics Purposes: to understand how users interact with the Platform, including feature usage, module usage, navigation patterns, user journeys, error patterns, adoption trends and customer requirements;

(d) Security Purposes: to detect suspicious activity, unauthorised access, misuse, abuse, fraud, security incidents and breaches of our terms; and

(e) Marketing Purposes: to measure engagement with our Website, marketing communications, campaigns and events, where permitted by applicable law.

Where required by applicable law, we will obtain consent before using non-essential cookies or similar technologies. You may be able to manage cookie preferences through your browser settings, device settings, cookie banner or other preference tools made available by us.

Strictly necessary cookies and similar technologies may be required for the Website or Platform to function properly. If you disable such technologies, certain features may not be available or may not operate correctly.

10.1 Managing Your Cookie Preferences

On your first visit to our website, you will be presented with a Cookie Consent Banner through which you may accept or decline non-essential Cookies. You may update your preferences at any time by clicking the "Cookie Settings" link in the footer of our website.

You may also control Cookies through your browser settings. Please note that disabling certain Cookies may affect the functionality of our website. Browser-level Cookie controls do not apply to Cookies set within the authenticated Platform environment.

10.2 Do Not Track

Some browsers transmit "Do Not Track" (DNT) signals to websites. We currently do not alter our data collection practices in response to DNT signals, as there is no universally accepted standard for DNT. We will revisit this position as standards develop.

11. Your Data Protection Rights

11.1 Rights of Data Subjects

Where we process your personal data on behalf of a business customer, we may not be the party that determines how and why your personal data is collected or used. In such cases, the relevant customer is generally responsible for responding to your request.

If you submit a request to us in relation to personal data that we process on behalf of a customer, we may:

(a) direct you to contact the relevant customer;

(b) notify the relevant customer of your request;

(c) seek instructions from the relevant customer before responding; and/or

(d) provide reasonable assistance to the relevant customer in responding to your request, where required by applicable law or contract.

We may be unable to respond directly to your request where doing so would conflict with the customer's instructions, affect the rights of other individuals, compromise security, disclose confidential information, or breach applicable law.

Subject to applicable law and certain limitations, individuals whose personal data we process have the following rights:

Right	Description	How to Exercise
Access	Request a copy of personal data we hold about you, together with information on how it has been used or disclosed, subject to applicable exceptions. Where we process your personal data on behalf of a customer, we may refer your request to that customer or seek that customer's instructions.	Submit a written request to privacy@udd.tech or contact the relevant customer where your data is processed through that customer's use of the Platform.
Correction	Request correction of inaccurate or incomplete personal data, subject to applicable law. Where your account or profile is managed by a customer, the customer may need to make or approve the correction.	Via account settings, by contacting privacy@udd.tech, or by contacting the relevant customer.

Right	Description	How to Exercise
Deletion (Erasure)	Request deletion of personal data where there is no overriding legal, contractual, security, audit, compliance or business reason for continued retention. Where we process your personal data on behalf of a customer, the customer may be responsible for determining whether deletion is appropriate.	Contact privacy@udd.tech or the relevant customer.
Restriction of Processing	Request that we restrict processing of your personal data in certain circumstances (GDPR).	Contact privacy@udd.tech
Data Portability	Receive your personal data in a structured, machine-readable format, where technically feasible (GDPR).	Contact privacy@udd.tech
Object to Processing	Object to processing based on legitimate interests or for direct marketing purposes.	Contact privacy@udd.tech or use unsubscribe links
Withdraw Consent	Withdraw consent where we rely on consent for the relevant processing activity. Withdrawal of consent does not affect processing carried out before withdrawal. Where consent was obtained by a customer, you should contact that customer to withdraw consent.	Contact privacy@udd.tech, use in-product controls where available, or contact the relevant customer.
Opt-Out of Marketing	Opt-out of marketing communications at any time.	Use the unsubscribe link in our emails or contact privacy@udd.tech

Right	Description	How to Exercise
Lodge a Complaint	Lodge a complaint with the relevant supervisory authority (PDPC in Singapore; applicable DPA in EEA/UK).	See contact details of supervisory authorities below

11.2 Requests from End Users

Where personal data is processed by UDD Technologies as a Data Processor on behalf of a Customer, End User rights requests should be directed in the first instance to the relevant Customer (as Data Controller). If you are unable to reach the Customer, you may contact us at privacy@udd.techand we will forward your request to the appropriate Customer and provide reasonable assistance.

11.3 Response Timeframes

- We will acknowledge receipt of your request within five (5) business days.
- We will respond substantively within thirty (30) calendar days of receipt.
- Where a request is complex or involves multiple data categories, we may extend this period by a further thirty (30) days, with prior notice.
- We reserve the right to verify the identity of the requester before fulfilling any access, correction, or deletion request.

11.4 Supervisory Authorities

- **Singapore — Personal Data Protection Commission (PDPC):** www.pdpc.gov.sg | +65 6377 3131
- **European Economic Area:** The competent Data Protection Authority in your EU member state.

12. Children's Personal Data

The Website and AthenaSpace Platform are not directed at and are not intended for use by individuals under the age of eighteen (18) years. We do not knowingly collect personal data from children under the age of eighteen (18).

If you believe that we have inadvertently collected personal data from a minor, please contact us immediately at privacy@udd.tech and we will take prompt steps to delete such data from our systems.

13. Customer Responsibilities

The AthenaSpace Platform is provided to business customers who determine how the Platform is configured and used within their own environments.

Our business customers are responsible for:

(a) determining which Platform modules, features and integrations are enabled;

(b) determining what personal data is collected, uploaded, generated or processed through their use of the Platform;

(c) determining which Customer Users, administrators and other personnel are granted access to the Platform;

(d) configuring access rights, roles, permissions, retention settings, integrations and workflows within the Platform;

(e) providing all notices and obtaining all consents or establishing all other lawful bases required for the collection, use, disclosure and processing of personal data through the Platform;

(f) informing employees, visitors, invitees, contractors, occupants and other End Users how their personal data may be collected and used through the customer's deployment of the Platform;

(g) ensuring that their use of the Platform complies with applicable laws, employment policies, workplace surveillance requirements, data protection requirements, internal governance requirements and contractual obligations; and

(h) ensuring that personal data submitted to or processed through the Platform is accurate, lawful and limited to what is necessary for the customer's intended purposes.

Where you are an End User of one of our business customers, you should review that customer's privacy notice or contact that customer directly to understand how your personal data is collected and used through its deployment of the Platform.

14. Third-Party Links and Integrations

Our Website and Platform may contain hyperlinks to third-party websites, applications, or services that are not operated by UDD Technologies. Such links are provided for reference and convenience only and do not constitute an endorsement of those third parties.

The AthenaSpace Platform may also offer integrations with third-party applications (e.g., Microsoft 365, Google Workspace, room booking systems, third-party content providers) enabled at the Customer's direction. Once data is transmitted to a third-party application, that party's own privacy policy and terms govern their collection and use of that data. We are not responsible for the privacy practices or content of third-party services.

We encourage you to review the privacy policies of any third-party services before providing them with your personal data.

15. Changes to this Privacy policy

We may revise this Privacy policy periodically. UDD Technologies reserves the right to update or modify this Privacy Policy at any time and from time to time without prior notice. Please review this policy periodically, and especially before you use our Sites or our Services or engage with our Marketing Activities. This Privacy Policy was last updated on the date indicated above.

16. Contact Us

Please feel free to contact us if you have any questions or concerns about our Privacy Policy.

Email us at privacy@udd.tech or contact us at below address:

Attention to: Internal Audit & Compliance Department

UDD Technologies Pte. Ltd.

16 Kallang Place, #06-07,

Singapore 339156

Contact number: +65 6741 4644