ALUMNI-Ready Data Protection Statement for University Clients

Effective Date: 11 May 2026
Last Updated: 11 May 2026

1. Purpose of this Statement

This Data Protection Statement explains how AppliedHE Pte. Ltd. (“AppliedHE”, “we”, “us”, or “our”) handles personal data when delivering the ALUMNI-Ready platform (the “Platform”) to university client institutions (each a “University Client”).

This Statement is published to provide transparency to University Clients, their alumni, and their internal compliance, legal and IT teams about the data protection measures AppliedHE applies in connection with the Platform.

This Statement should be read together with the ALUMNI-Ready Privacy Policy and the ALUMNI-Ready Terms of
Service. The Terms of Service govern the contractual relationship between AppliedHE and each University Client.

This Statement is provided for transparency and information purposes only. It does not create additional contractual obligations, warranties, guarantees, service levels, indemnities, or liabilities beyond those expressly set out in the Terms of Service or required under applicable law.

2. Roles and Responsibilities Under the PDPA

ALUMNI-Ready is a software-as-a-service platform. AppliedHE provides the software, infrastructure and technical operation of the Platform. The University Client uses the Platform as a tool to manage its own alumni community.

The University Client retains full control over all personal data within its own Platform instance, including decisions about:

What data is collected.

Why the data is collected.

How the data is used.

Who the data is shared with.

How long the data is retained.

How requests from individuals are handled.

Under the Personal Data Protection Act 2012 of Singapore (“PDPA”):

The University Client is the Organisation in respect of all personal data uploaded into, collected through, or generated by its Platform instance. The University Client is responsible for fulfilling all obligations of an Organisation under the PDPA and any other applicable data protection laws. This includes obtaining consents, providing notifications, managing withdrawals of consent, responding to access and correction requests, and ensuring that its use of the Platform is lawful.

AppliedHE acts as a Data Intermediary in respect of personal data processed on behalf of the University Client. AppliedHE processes such data only to provide, maintain, secure and support the Platform.

AppliedHE does not determine the purposes for which the University Client collects or uses personal data, and AppliedHE does not control the University Client’s communications, alumni engagement activities, fundraising activities, job postings, events, or other use of the Platform.

3. Categories of Personal Data Processed

The Platform may process the following categories of personal data on behalf of a University Client:

Identification data, such as names, email addresses, phone numbers and mailing addresses.

Academic records, such as graduation year, faculty, programme, student number, alumni ID and other institutional records.

Professional information, such as employer, role, industry, professional location and career history.

Profile content, such as profile photos, biographies and links to professional or social media profiles.

Engagement and usage data, such as logins, page interactions, event attendance, group membership and platform activity.

Communications, such as posts, comments, direct messages, news submissions and success stories.

Event and membership records, such as registrations, ticket purchases, membership tier history and RSVP responses.

Job board records, such as job listings posted by alumni or employers and applications submitted through the Platform.

Donation, sponsorship and payment-related records, where such functions are used by the University Client.

Custom fields, including any additional data fields configured by the University Client through the Platform.

The exact data set held in each Platform instance is determined by the University Client. AppliedHE is not responsible for the University Client's decision to collect any specific category of personal data.

4. Limited Processing and No Access in the Ordinary Course

AppliedHE's processing of personal data on behalf of a University Client is limited to what is necessary to operate the Platform as a software service.

4.1 What AppliedHE Does With Customer Data

AppliedHE may process Customer Data to:

Store personal data on behalf of the University Client.

Transmit personal data between authorised users of the Platform.

Maintain the security, availability and integrity of the Platform.

Perform routine backups, system maintenance and disaster recovery operations.

Provide technical support to authorised University Client administrators where requested.

Generate aggregated or anonymised statistics that do not identify any individual.

Diagnose technical issues, fix bugs and improve Platform performance.

Comply with applicable legal or regulatory obligations.

4.2 No Access in the Ordinary Course

AppliedHE personnel do not access, view or read personal data held on behalf of a University Client in the ordinary course of operating the Platform.

Access by AppliedHE personnel is limited to specific circumstances, including:

Customer-initiated support, where the University Client requests assistance and access to limited data is reasonably necessary to diagnose or resolve an issue.

Security and abuse investigations, where AppliedHE investigates a security incident, fraud, abuse, misuse, unauthorised access, or a credible threat to the Platform.

Maintenance and technical operations, where limited access is required to maintain service integrity, backup systems, restore functionality, or resolve technical errors.

Legal or regulatory obligations, where AppliedHE is required by law, court order, regulator, or competent authority to access or disclose specific data.

Where access occurs, AppliedHE will apply least-privilege principles and reasonable access controls.

4.3 No Secondary Use of Customer Data

AppliedHE does not use personal data held on behalf of a University Client for purposes unrelated to providing and supporting the Platform.

AppliedHE does not:

Sell, rent, licence, or trade Customer Data.

Use Customer Data for AppliedHE's own marketing or advertising.

Use Customer Data to build individual profiles outside the Platform.

Use Customer Data to train artificial intelligence or machine learning models.

Disclose Customer Data to third parties except as described in this Statement, the Privacy Policy, the Terms of

Service, or as required by law.

4.4 Ownership

Customer Data remains the property of the University Client or, where applicable, the individual data subject.

AppliedHE does not claim ownership of Customer Data.

5. University Client Responsibilities

The University Client is responsible for its own compliance with applicable data protection, privacy, marketing, communications, fundraising, employment, consumer protection and sector-specific laws.

The University Client is responsible for:

Obtaining all required consents from alumni, students, staff, donors, employers, event participants and other individuals.

Providing appropriate privacy notices to individuals.

Ensuring that personal data uploaded to the Platform has been lawfully collected.

Ensuring that personal data is accurate, relevant and up to date.

Managing withdrawals of consent.

Responding to access, correction, deletion, objection and other data subject requests.

Managing End User permissions and administrator access.

Moderating content posted within its Platform instance.

Ensuring that communications sent through the Platform comply with applicable laws.

Ensuring that fundraising, donation, sponsorship, event, payment and job board activities are lawful.

Configuring the Platform appropriately for its intended use.

AppliedHE is not responsible for the University Client's use of the Platform, the lawfulness of Customer Data, the content uploaded by users, or the University Client's communications, events, fundraising, alumni relations, job postings, sponsorship activities, or payment arrangements.

6. Hosting Location and Cross-Border Transfers

Personal data processed through the Platform is currently hosted on infrastructure located in Singapore, provided by DigitalOcean LLC.

AppliedHE does not routinely transfer Platform personal data outside Singapore.

If a cross-border transfer becomes necessary in the future, AppliedHE will take reasonable steps to ensure that the recipient is bound by legally enforceable obligations providing a standard of protection comparable to that under the PDPA, where required by applicable law.

Where a University Client chooses to connect the Platform with an external service, the University Client is responsible for assessing and managing any cross-border transfers associated with that external service.

7. Technical and Organisational Security Measures

AppliedHE implements reasonable technical and organisational measures designed to protect personal data against unauthorised access, collection, use, disclosure, copying, modification, disposal, loss, or similar risks.

These measures may include the following:

7.1 Network and Transport Security

Connections to the Platform are encrypted using TLS.

SSL certificates are provisioned and maintained for Platform domains where applicable.

Production servers are protected by firewalls and restricted access rules.

7.2 Authentication and Access Controls

Passwords are stored as one-way cryptographic hashes.

Two-factor authentication may be available for administrator accounts.

Role-based access controls govern administrator permissions within the Platform.

Access to production systems by AppliedHE personnel is restricted on a need-to-know basis.

Administrative access uses secure authentication methods.

7.3 Data Isolation

Each University Client operates within a logically isolated Platform environment.

University Client data is separated using application-level and database-level controls where applicable.

One University Client is not permitted to access another University Client's data.

7.4 Audit and Monitoring

Administrative actions may be logged.

Authentication events and system activity may be monitored.

Anomalous activity may be reviewed by AppliedHE technical staff.

Logs may be retained for a defined period to support security, troubleshooting and incident investigation.

7.5 Software and Infrastructure Hygiene

Application dependencies are monitored and updated where appropriate.

Security patches are applied through controlled maintenance processes.

Production deployments follow internal review and change management practices.

7.6 Backup and Disaster Recovery

Database backups are performed regularly.

Backups are stored within the Singapore region where practicable.

Backup integrity may be checked periodically.

Backup copies are retained according to AppliedHE's technical retention and rotation practices.

7.7 Personnel Measures

AppliedHE personnel with access to production systems are subject to confidentiality obligations.

Personnel handling personal data receive guidance on data protection responsibilities.

Access rights are reviewed and revoked where no longer required.

No system, network, software, infrastructure, or transmission method can be guaranteed to be completely secure, uninterrupted, or error-free. AppliedHE does not warrant absolute security.

8. Sub-Processors and Third-Party Services

AppliedHE currently engages the following sub-processor in delivering the Platform:

Sub-processor: DigitalOcean LLC

Role: Cloud infrastructure, including compute, storage, networking and managed databases

Location: Singapore

AppliedHE does not currently send University Client data to third-party email delivery services, payment processors, analytics platforms, advertising platforms, or artificial intelligence services as part of the core Platform service, unless otherwise notified or agreed.

AppliedHE may change or appoint sub-processors from time to time as reasonably necessary to operate, maintain, secure, improve, or support the Platform. Where a new sub-processor will process personal data on behalf of University Clients, AppliedHE will provide reasonable notice where practicable.

Where a University Client chooses to integrate the Platform with external services, including email services, payment gateways, analytics tools, SMS providers, authentication services, job portals, or other third-party systems, the University Client is responsible for that external service.

AppliedHE is not responsible for:

The availability, reliability, performance, security, or legality of third-party services selected by the University Client.

The privacy practices or data handling of those third-party services.

Any fees, errors, losses, disputes, data breaches, or claims arising from such third-party services.

Any data shared by the University Client or End Users with those third-party services.

9. Data Breach Management and Response

AppliedHE applies commercially reasonable measures designed to reduce the likelihood and impact of security incidents. However, personal data breaches may occur despite reasonable safeguards.

This section describes AppliedHE's intended response process in the event of a suspected or confirmed personal data breach affecting the Platform.

9.1 Definition of Personal Data Breach

A personal data breach includes unauthorised access to, collection, use, disclosure, copying, modification, disposal, or loss of personal data, or any similar incident involving personal data.

9.2 Detection and Initial Response

AppliedHE may detect or receive notice of a suspected breach through monitoring, logs, administrator reports, third-party reports, security reviews, or other sources.

When AppliedHE becomes aware of a suspected breach, it will take reasonable steps to:

Review the available information.

Contain the incident where practicable.

Preserve relevant evidence and logs.

Investigate the nature and scope of the incident.

Assess whether Customer Data may have been affected.

9.3 Investigation and Assessment

AppliedHE will take reasonable steps to assess:

The cause and nature of the incident.

The affected systems or Platform components.

The categories of personal data potentially affected.

The University Client or University Clients potentially affected.

The approximate number of individuals affected, where reasonably ascertainable.

The likely risk of harm, where reasonably ascertainable.

9.4 Notification to University Client

Where AppliedHE confirms that a personal data breach has occurred affecting a University Client's Customer Data, AppliedHE will notify the affected University Client without undue delay, where required by applicable law or contract.

The notification may include, to the extent reasonably available:

A summary of the incident.

The categories of data affected.

The approximate number of affected records or individuals, where known.

Containment steps taken.

Recommended actions for the University Client.

A contact point for follow-up.

Where full details are not available at the time of initial notification, AppliedHE may provide information in stages as the investigation progresses.

9.5 Statutory Notifications

For Customer Data held in a University Client's Platform instance, the University Client is responsible for assessing and making any required notification to affected individuals, regulators, authorities, or other parties.

AppliedHE will provide reasonable cooperation to the University Client where required and practicable.

AppliedHE does not make statutory notifications on behalf of a University Client unless expressly agreed in writing or required by law.

Where the affected data is personal data for which AppliedHE is the Organisation, AppliedHE will assess and make any required notifications in accordance with applicable law.

9.6 Containment and Remediation

AppliedHE may take steps to:

Complete containment of the incident.

Apply corrective measures.

Conduct root-cause analysis.

Implement security improvements where appropriate.

Document the incident and response.

9.7 Post-Incident Report

Where appropriate, and taking into account the nature and impact of the incident, AppliedHE may provide the affected University Client with a written post-incident summary.

The summary may include:

The nature of the incident.

The data affected.

Actions taken.

Remediation steps.

Recommendations for the University Client where relevant.

9.8 No Admission of Liability

Nothing in this Statement, any breach notification, any incident report, or any cooperation provided by AppliedHE constitutes:

An admission of liability or wrongdoing by AppliedHE.

A warranty of absolute security.

A waiver of any right, defence, immunity, exclusion, or limitation of liability available to AppliedHE.

An undertaking to perform obligations beyond those required by applicable law, the Terms of Service, or a written agreement with the University Client.

AppliedHE's liability, if any, remains subject to the limitations and exclusions set out in the Terms of Service and applicable law.

10. Assistance with Data Subject Rights

The PDPA gives individuals certain rights, including access, correction and withdrawal of consent.

For Customer Data held in a University Client's Platform instance, these rights should be exercised against the University Client, as the Organisation responsible for that data.

The University Client has administrative tools that may allow it to:

Search, view and export an individual's records.

Edit or correct personal data.

Delete an individual's account or associated data.

Manage communication preferences.

Manage consent-related fields.

Export personal data where available.

AppliedHE does not handle data subject requests directly for Customer Data controlled by a University Client, unless required by law or expressly instructed by the University Client.

AppliedHE may provide reasonable technical assistance to the University Client where a request cannot be resolved using standard Platform tools.

11. Retention and Deletion

Personal data is retained only for as long as necessary for the purposes for which it was collected, or as required or

permitted by law.

For Customer Data held in a University Client's Platform instance, the University Client determines the applicable retention period.

Upon termination of a University Client's subscription or use of the Platform, AppliedHE will handle Customer Data in accordance with the Terms of Service and any applicable written agreement.

AppliedHE may, where technically feasible and subject to applicable law:

Return Customer Data to the University Client in a portable format.

Delete Customer Data from active systems.

Retain backup copies for a limited period in accordance with standard backup rotation practices.

Retain data where required for legal, security, audit, dispute resolution, or compliance purposes.

A certificate of deletion may be provided on written request where reasonably practicable.

12. Confidentiality

AppliedHE treats Customer Data as confidential information.

AppliedHE will not disclose Customer Data except:

To the University Client and its authorised personnel.

To AppliedHE personnel, contractors, advisers and service providers who need access for authorised purposes and are subject to confidentiality obligations.

To DigitalOcean LLC or other approved infrastructure or service providers where necessary to provide the Platform.

Where required by law, court order, regulator, authority, or legal process.

Where necessary to protect the rights, safety, security, property, or legal interests of AppliedHE, University Clients, End Users, or others.

With the University Client's written consent.

13. Audit and Verification

AppliedHE may, on reasonable written request and no more than once per calendar year, provide a University Client with reasonable information to demonstrate AppliedHE's data protection measures.

This may include:

Written responses to a reasonable data protection questionnaire.

General documentation describing security controls.

Information reasonably necessary to demonstrate the measures described in this Statement.

AppliedHE is not required to provide access to its production systems, source code, confidential business information, security-sensitive information, information relating to other clients, or information that would compromise the security or confidentiality of AppliedHE or any third party.

Any audit, review, or information request must be conducted in a manner that does not unreasonably disrupt AppliedHE's operations and is subject to confidentiality obligations.

More frequent reviews may be considered where required to investigate a confirmed security incident affecting the University Client's data.

14. Limitation and Allocation of Responsibility

AppliedHE provides the Platform as a software-as-a-service tool and does not control how the University Client chooses to use it.

AppliedHE is not responsible for:

The accuracy, completeness, legality, or quality of Customer Data.

The University Client's lawful basis for collecting or using personal data.

The University Client's failure to obtain consent or provide required notices.

The University Client's communications, marketing, fundraising, event, payment, donation, sponsorship, job board, or alumni engagement activities.

Content posted or shared by Administrators or End Users.

Misuse of the Platform by the University Client, Administrators, End Users, or third parties.

Security incidents caused by the University Client's systems, devices, credentials, configurations, integrations, or third-party services.

Any outcome, revenue, donation, sponsorship, event participation, alumni engagement result, employability result, ranking improvement, or institutional benefit expected from use of the Platform.

AppliedHE's liability, if any, is limited as set out in the ALUMNI-Ready Terms of Service and applicable law.

15. Governing Law

This Statement is governed by the laws of Singapore.

The Platform's processing of personal data is subject to the PDPA and applicable regulations and guidelines issued by the PDPC.

Where a University Client is established in another jurisdiction, the University Client remains responsible for complying with the data protection, privacy and other applicable laws of that jurisdiction.

AppliedHE may provide reasonable assistance where such assistance is within the scope of the Platform, the Terms of Service and applicable law.

16. Updates to this Statement

AppliedHE may update this Statement from time to time to reflect changes in law, regulatory guidance, infrastructure, security measures, Platform features, business operations, or data handling practices.

The "Last Updated" date at the top of this Statement indicates when it was last revised.

Where changes are material, AppliedHE will provide reasonable notice to active University Clients through email, the Platform, or other appropriate means.

Continued use of the Platform after an updated Statement takes effect constitutes acknowledgement of the updated Statement.

17. Contact

For questions about this Statement or AppliedHE's handling of personal data in connection with the Platform, please contact:

Data Protection Contact

AppliedHE Pte. Ltd.

7 Temasek Boulevard

#12-07 Suntec Tower One

Singapore 038987

Email: privacy@appliedhe.com

For general enquiries, please contact:

AppliedHE Pte. Ltd.

Email: info@appliedhe.com

University Clients are encouraged to direct compliance enquiries, data protection questions, audit requests and breach-related communications to the Data Protection Contact.

18. Relationship with Terms of Service

This Statement is provided for transparency and information purposes only.

It does not, by itself, constitute a contract between AppliedHE and any University Client.

The contractual terms governing access to and use of the Platform are set out in the ALUMNI-Ready Terms of Service, any applicable order form, invoice, proposal, subscription plan, or written agreement accepted by the University Client.

If there is any inconsistency between this Statement and the Terms of Service or any written agreement between AppliedHE and the University Client, the Terms of Service or written agreement shall prevail to the extent of the

inconsistency, unless otherwise required by applicable law.