TeamRetro

GroupMap Technology Pty Ltd.

SOC 3 for Service Organization Reports

1 March 2024 to 28 February 2025

Contents

Section I

ASSERTION OF GROUPMAP TECHNOLOGY PTY LTD MANAGEMENT

ASSERTION OF GROUPMAP TECHNOLOGY PTY LTD MANAGEMENT

28 April 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within GroupMap Technology Pty Ltd.'s ('GroupMap Technology') TeamRetro Software as a Service System (the 'System') throughout the period 1 March 2024 to 28 February 2025 to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality and Privacy ('Agreed Criteria') set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in 'GroupMap Technology's Description of its System' (the 'Description') and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period 1 March 2024 to 28 February 2025 to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the Agreed Criteria. GroupMap Technology's objectives for the system in applying the Agreed Criteria are embodied in its service commitments and system requirements relevant to the Agreed Criteria. The principal service commitments and system requirements related to the Agreed Criteria are presented in 'GroupMap Technology's Description of its System.'

GroupMap Technology uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GroupMap Technology, to achieve GroupMap Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap Technology's controls, the Agreed Criteria, and the types of complementary subservice organization controls assumed in the design of GroupMap Technology's controls. The Description does not disclose the actual controls at the subservice organization.

The Description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at GroupMap Technology, to achieve GroupMap Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap Technology's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of GroupMap Technology's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period 1 March 2024 to 28 February 2025 to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the Agreed Criteria.

Jeremy Lu
Chief Executive Officer
GroupMap Technology Pty Ltd

Section II

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: GroupMap Technology Pty Ltd.

Scope

We have examined GroupMap Technology Pty Ltd.'s ('GroupMap Technology') accompanying description of its TeamRetro Software as a Service System titled "GroupMap Technology Pty Ltd.'s Description of Its TeamRetro Software as a Service System" throughout the period 1 March 2024 to 28 February 2025, (the 'Description') based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report (With Revised Implementation Guidance — 2022) in AICPA, Description Criteria, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period 1 March 2024 to 28 February 2025, to provide reasonable assurance that GroupMap Technology 's service commitments and system requirements were achieved based on the trust services criteria for security, availability, confidentiality and privacy (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022) in AICPA, Trust Services Criteria.

GroupMap Technology uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GroupMap Technology, to achieve GroupMap Technology's service commitments and system requirements based on the Agreed Criteria. The complementary subservice organization controls have been reviewed by GroupMap Technology management. The Description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description includes complementary user entity controls that are necessary, along with controls at GroupMap Technology, to achieve GroupMap Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents GroupMap Technology's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of GroupMap Technology's controls. The complementary user entity controls have not been assessed by our examination and remain the responsibility of those related entities to complete their own review.

Service Organization's Responsibilities

GroupMap Technology is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved. GroupMap Technology has provided the accompanying assertion titled "Assertion of GroupMap Technology Pty Ltd Management" (the 'Assertion') about the Description and the suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the Agreed Criteria. GroupMap Technology is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable Agreed Criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the GroupMap Technology's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of controls stated in the Description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and in accordance with International Standard on Assurance Engagements

3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board.

- The Description is presented in accordance with the Description Criteria.
- The controls stated in the Description were suitably designed.
- The controls stated in the Description were operating effectively throughout the period to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the Agreed Criteria.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the Description of GroupMap Technology's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the System and GroupMap Technology's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that GroupMap Technology achieved its service commitments and system requirements based on Agreed Criteria.
- Testing the operating effectiveness of controls stated in the Description to provide reasonable assurance that GroupMap Technology achieved its service commitments and system requirements based on the Agreed Criteria.
- Evaluating the overall presentation of the Description.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

Because of the inherent limitations of any internal control structure, it is possible that, even if the controls are suitably designed and operating effectively, the control objectives may not be achieved, and so fraud, error, or non-compliance with laws and regulations may occur and not be detected.

An assurance engagement on the operating effectiveness of controls is not designed to detect all instances of controls operating ineffectively as they are not performed continuously throughout the period, and the tests performed are on a sample basis. Any projection of the outcome of the evaluation of controls to future periods is subject to the risk that the controls may become inadequate because of changes in conditions or that the degree of compliance with them may deteriorate.

Opinion

In our opinion, management's assertion that the controls within GroupMap Technology's TeamRetro Software as a Service System were effective throughout the period 1 March 2024 to 28 February 2025, to provide reasonable assurance that GroupMap Technology's service commitments and system requirements were achieved based on the Agreed Criteria is fairly stated, in all material respects.

AssuranceLab CPAs LLC
Austin, Texas
United States
28 April 2025

Section III

GROUPMAP TECHNOLOGY PTY LTD'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF OPERATIONS

Company Background

GroupMap Technology Pty Ltd ('GroupMap Technology') is an Australian-based, globally distributed software company founded in September 2012. Headquartered in Perth, Western Australia, the organization develops and delivers web-based Software-as-a-Service (SaaS) solutions designed to facilitate collaboration, inform decision-making, and enhance productivity. The company's products—most notably TeamRetro—are used by a wide range of organizations, from small startups to multinational enterprises. GroupMap Technology supports customers across Australia, New Zealand, Asia, the United States and Europe.

The company serves a diverse range of industries, including:

- Information Technology
- Professional Services
- Financial Services
- Healthcare
- Government
- Defense
- Education
- Telecommunications
- Manufacturing
- Pharmaceutical
- Gaming and Entertainment
- Consumer Goods

The company employs a distributed workforce, leveraging modern cloud technologies and agile development practices to provide services to its global customer base. Tools such as TeamRetro offer structured support for retrospectives, health checks, and other collaborative activities, enabling teams to maintain continuous improvement across diverse operational contexts.

Description of Services Provided

TeamRetro is GroupMap Technology's core web-based application, designed for agile teams to conduct structured retrospectives and team health checks. By facilitating structured collaboration, TeamRetro enables organizations to manage continuous improvement, track action items, and understand team sentiment and challenges.

Key Features and Functions

Retrospective Meetings:

- Prompts and Templates: Users can select or customize retrospective templates (e.g., "What Went Well?", "What Didn't Go Well?") to capture observations, ideas, and feedback.
- Idea Capture and Grouping: Participants add ideas anonymously or with attribution, then group and consolidate similar items for efficient discussion.
- Voting and Prioritization: Team members vote to identify top priorities for deeper analysis.
- Discussion and Reactions: As items are discussed, participants can add reactions, comments, and clarifications in real time.
- Action Items and Team Agreements: Based on discussions, new action items or team agreements can be proposed, documented, and assigned.

- Summary Publishing: Meeting outcomes can be exported or shared with third-party tools (e.g., Confluence, Slack) to keep stakeholders informed.

Health Check Meetings:

- Health Dimensions: Users rate and comment on key health factors (e.g., Codebase Complexity, Communication, Teamwork) using built-in or custom templates.
- Sorting and Analysis: Overall results are aggregated and sorted, highlighting the dimensions most in need of attention or improvement.
- Collaborative Discussion: Teams discuss each dimension, adding further comments, action items, or team agreements.
- Final Review: Action items and agreements are finalized, assigned, and shared with participants.

Both retrospective and health check features can be run synchronously (live) or asynchronously, and teams can choose whether to conduct these sessions anonymously or with full attribution.

AI Features:

- Retrospective Template Generation: Offers structured retrospective templates aligned with agile methodologies
- Health Model Template Generation: Recommends health check dimensions based on industry best practices and team context
- Icebreaker Question Generation: Suggests relevant, engaging prompts for quick team warm-ups
- Meeting Summarization: Auto-creates concise summaries of discussions, decisions, and action items
- Suggested Grouping: Clusters similar ideas to speed up organization and reduce manual work
- Suggested Actions: Highlights potential tasks or improvements tied to meeting discussions
- Suggested Group Titles: Provides clear, concise labels for grouped ideas or themes
- Suggested Meeting Titles: Proposes memorable, context-specific names for sessions

Team Action Items:

- Creation and Status Tracking: Users can propose, create, update, and track the status of action items arising from retrospectives or health checks.
- Integration: Actions can be published directly to third-party task management systems (e.g., Jira, Trello, Azure DevOps).

Team Agreements:

- Proposal and Acceptance: Teams can propose and finalize agreements for improved ways of working.
- Visibility: Agreements are visible in team dashboards for easy reference and follow-up.

Reporting and Analytics:

- Cross-Team Insights: High-level dashboards highlight usage trends, health metrics, and retrospective outcomes, and key sentiments across multiple teams.
- Activity and User Reports: Detailed logging and exports (PDF, CSV, XLSX) help visualize participation and track progress on items over time.
- API and SCIM: Offers programmatic access and provisioning capabilities for advanced integration with enterprise systems.

Principal Service Commitments and System Requirements

GroupMap Technology designs its processes and procedures related to its TeamRetro Software as a Service System (the 'System') to meet its objectives. Those objectives are based on the service commitments that GroupMap Technology makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational, and compliance requirements that GroupMap Technology has established for the services. Security commitments to user entities are documented and communicated in service level agreements and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include security principles within the fundamental designs of the Software as a Service System that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.

GroupMap Technology establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in GroupMap Technology's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. GroupMap Technology is committed to delivering secure, high-performing services that meet the needs of diverse user entities. The company's processes, procedures, and controls for the System are designed to fulfill the following obligations:

Service Commitments

- Performance and Reliability: The System's architecture and operational procedures aim to provide high availability and rapid response times.
- Security and Privacy: The System's security posture is governed by robust administrative, technical, and physical safeguards. Controls are documented in Data Processing Agreements, enterprise agreements, and the publicly available TeamRetro Privacy Policy.
- Regulatory and Contractual Compliance: GroupMap Technology's System adheres to applicable laws, regulations, and contractual obligations, including industry standards like SOC 2, which governs the internal controls over security, confidentiality, and privacy.

User Access and Licensing

- Terms of Service (TOS): All users must abide by the TeamRetro TOS, which prohibits sub-licensing or unauthorized account sharing. Each user must have a valid license or be invited under a license holder's account.
- Enterprise Agreements: In some cases, enterprise customers may have separate agreements or service level agreements (SLAs) that override portions of the standard TOS. Where such agreements exist, those terms govern in the event of any conflict.

Security Commitments

- Principle-Based Architecture: The System's fundamental design restricts access to data based on a user's role, ensuring that only authorized individuals can view or modify information.
- Documentation and Communication: Security obligations are clearly explained in Data Processing Agreements, enterprise contracts, and the System's service description.
- Standardized Policies: All security commitments—ranging from encryption standards to incident response procedures—are formalized and maintained centrally, aligned with relevant regulatory requirements.

Operational Requirements

- Policies and Procedures: The company's internal policies define how the service is designed and developed, how the system is operation, how the internal business systems and networks are managed, how employees are hired and trained, and how data are protected at every stage—from

design and development to deployment and day-to-day operations. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the System.

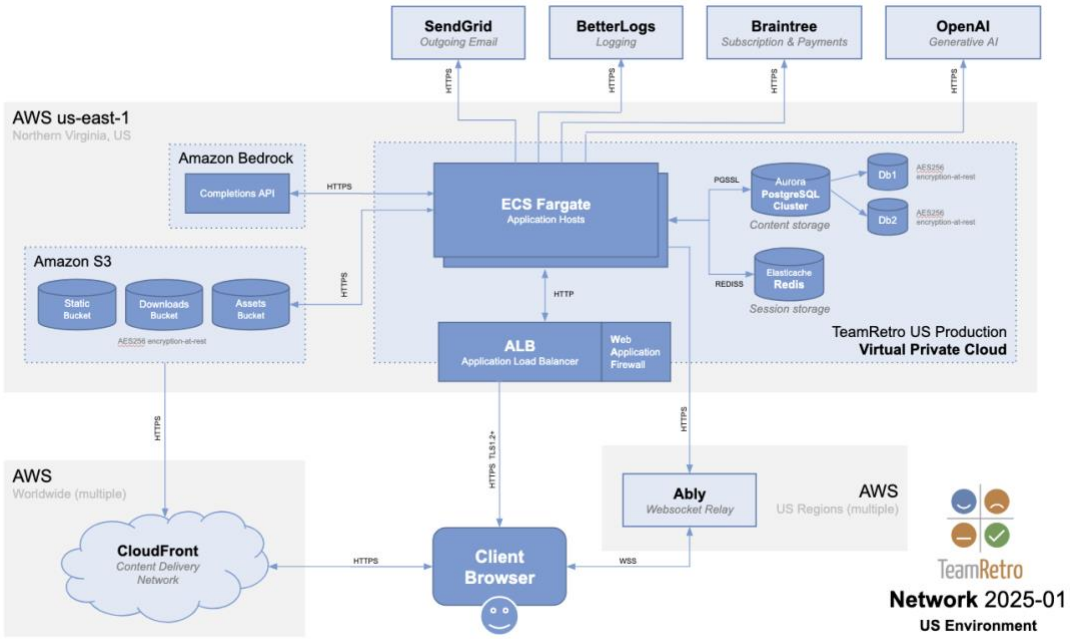
- Employee Training and Management: Stringent hiring, onboarding, and training practices ensure that employees understand and adhere to established security and operational protocols.
- Standard Operating Procedures (SOPs): Well-documented SOPs outline the manual and automated processes essential for operating and developing the System, including secure coding practices, patch management, and data backup routines.

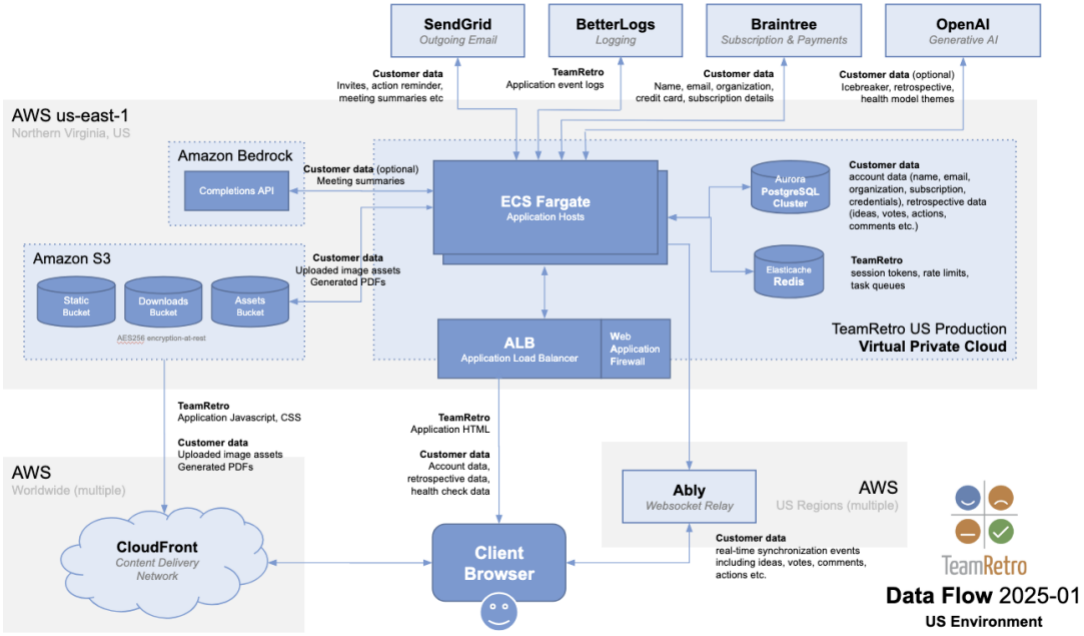
Components of the System

This section provides an overview of the technical components and third-party services that power the System. It covers the primary hosting environment, sub-processors responsible for infrastructure and platform services, additional software used for operations, and the safeguards in place to protect data.

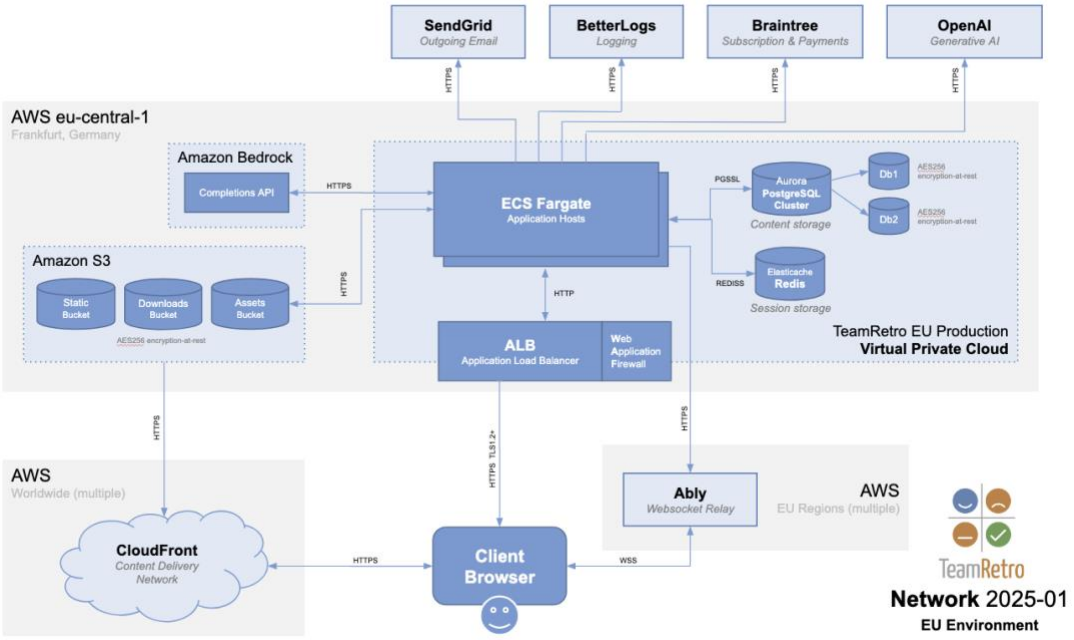
System Architecture

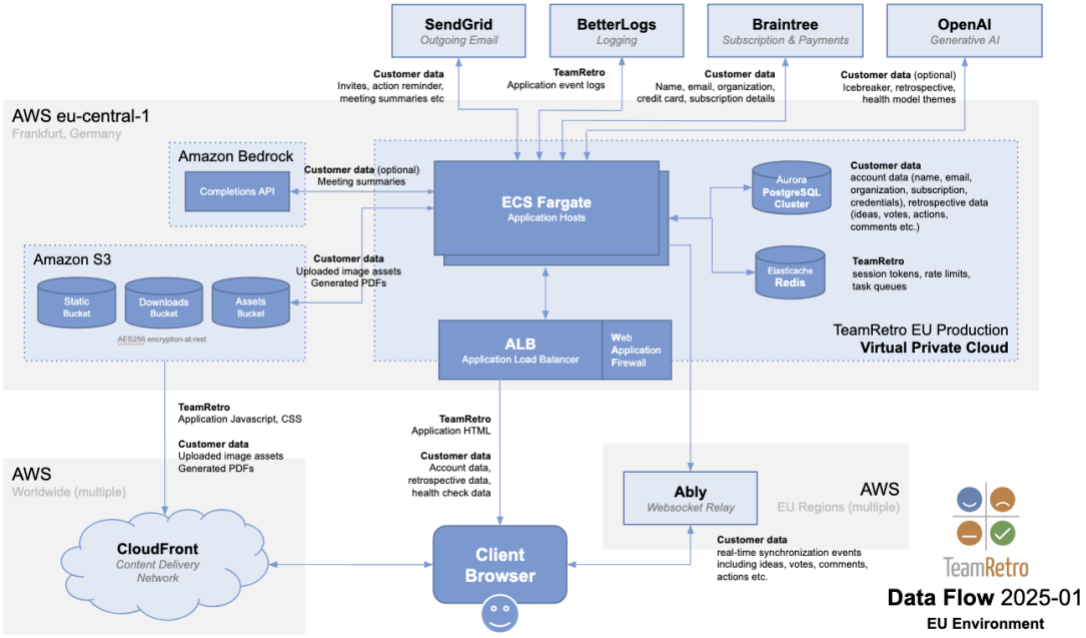
TeamRetro US Environment





TeamRetro EU Environment





The following principles guide the design and operation of the System's architecture:

- Scalability: Containerized services and managed databases allow seamless scaling to handle varying workloads and user demands.
- Resilience: Critical components are redundantly hosted across AWS Availability Zones, safeguarding continuity if a primary component fails.
- Security by Design: Infrastructure, application, and data layers are configured with security at the forefront—encryption in transit and at rest, rigorous monitoring, and robust identity and access management (IAM).
- Compliance and Transparency: Regular reviews, third-party audits, and adherence to recognized standards (e.g., SOC 2) ensure that GroupMap Technology meets and exceeds customer and regulatory requirements.

Infrastructure

GroupMap Technology's primary infrastructure used to provide the System includes the cloud hosted networking, compute and database components of Amazon Web Services ('AWS'). The System utilizes AWS data centers in Northern Virginia, United States (us-east-1) and Frankfurt, Germany (eu-central-1). Together, these AWS components form the core of the System's service architecture, delivering scalable and resilient operations across multiple regions.

System	Type	Description
Amazon Elastic Compute Cloud (EC2)	Cloud Compute	Secure and resizable compute capacity (virtual servers) in the cloud.
Amazon Simple Storage Service (S3)	Data Storage	Object, file, and block storage.
AWS RDS (Aurora Postgres)	Data Storage	Fully managed, relational database service for storing and querying user data.

System	Type	Description
Amazon Simple Storage Service (S3)	Data Storage	Object, file, and block storage.
AWS Backup	Data Backup	Automates encrypted backups of customer data on a daily basis.
AWS Bedrock	Cloud Compute	Generative AI for content synthesis.
AWS ElastiCache (Redis)	Cloud Compute	Facilitates session management, rate-limiting, and caching to optimize performance.
AWS CloudFormation	Cloud Compute	Management tool used to model, provision and manage AWS and third-party resources through infrastructure as code.
AWS Key Management Service (KMS)	Key Management	Provides centralized control over the lifecycle and permissions of cryptographic keys to encrypt and protect data.
AWS CloudFront	Networking	Serves static assets to end users with low latency and high transfer speeds.
AWS Elastic Load Balancing (ELB)	Networking	Automatically distributes incoming application traffic across multiple targets.
AWS Virtual Private Cloud (VPC)	Networking	Dedicated virtual network to launch AWS resources in a logically isolated network.
AWS Route 53	Networking	Domain Name System (DNS) web service to route and manage DNS traffic within and outside of AWS.
AWS Web Application Firewall (WAF)	Network Protection	Protects against common web exploits by monitoring and filtering malicious traffic.
AWS CloudWatch	Network Monitoring	Monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources.
AWS CloudTrail	System Monitoring	Enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage on AWS.
AWS GuardDuty	Network & System Monitoring	Threat detection service that continuously monitors AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.

Software

GroupMap Technology also uses a range of software tools to manage internal operations and deliver the System service effectively. While these do not directly host customer-facing data, they are key to day-to-day business processes. Primary software used to support GroupMap Technology's System is defined as below:

Software	Purpose
TeamRetro	The Software as a Service product provided to GroupMap Technology customers.
Datadog, BetterUptime	System monitoring software used to log events and raise alerts to support system security and availability.
Intruder.io, Qualys	Vulnerability scanning software to identify, log and resolve technical vulnerabilities.
Codacy	Code review tool used to conduct static code analysis tool, monitor code quality and automate code reviews.
GitHub	Source code repository used to manage the software code and version control. Continuous integration / continuous delivery software used to manage the pipeline of change release testing and deployment.
1Password	Enterprise password manager used to store authentication secrets and strengthen password security.
Bitdefender	Anti-virus software used to protect endpoint devices from malware.
Hexanode MDM	Mobile device management software used to track and manage security policies on endpoint devices.
Xero	Accounting software used to track financial records, automate invoicing and bank reconciliations to support the financial operations.
Slack	Communication platform used to collaborate between team members and support business operations.
Ninjio	Security awareness training platform used to track and manage the internal training requirements.
Prighter	Privacy representation and compliance software used to manage privacy practices in line with data protection laws.
HelpScout	Customer support ticketing and knowledge base used to support and manage customer communication.
HelloNext	Feedback management tool used for product roadmap planning and customer feedback collection.
Linear	Ticketing software used to log events and requirements to support the internal controls.

Software	Purpose
Google Workspace	Google's suite of enterprise productivity, collaboration, and communication tools. Authentication software used to identify and authenticate users for access control to the systems.

People

GroupMap Technology is a globally distributed company with approximately 13 employees. The primary functional areas include:

Executive and Corporate
Scope: Executive leadership, finance, talent acquisition, human resources, and compliance.
Responsibilities:

- Develop and drive overall company strategy and vision.
- Manage financial operations, budgeting, and resource allocation.
- Oversee hiring, onboarding, and professional development.
- Ensure regulatory compliance and corporate governance.

Customer Experience (CX)
Scope: Customer support, customer success, and customer delivery.
Responsibilities:

- Provide day-to-day support and training for existing customers.
- Onboard new clients to ensure successful adoption of the TeamRetro Software as a Service System.
- Gather customer feedback and collaborate with product teams to enhance service quality.
- Drive continuous improvements in service delivery and user satisfaction.

Product Development
Scope: Product management, user experience (UX) design, software development, and quality assurance.
Responsibilities:

- Plan and prioritize product roadmaps based on customer feedback and market trends.
- Conduct design sprints, user research, and UX optimization.
- Implement and maintain application features, integrations, and system enhancements.
- Ensure consistent high quality through rigorous testing and QA processes.

Operations
Scope: Infrastructure, security, reliability engineering, and DevOps.
Responsibilities:

- Manage hosting environments, networking, and cloud-based infrastructure.
- Monitor system performance, capacity, and uptime to meet Service Level Objectives.
- Oversee data security, incident response, and platform resilience.
- Collaborate with development teams to streamline deployment pipelines and automation.

Sales
Scope: Business growth, customer retention, and strategic partnerships.
Responsibilities:

- Identify and cultivate new business opportunities across various industries.
- Maintain strong relationships with existing accounts, focusing on retention and expansion.
- Partner with marketing to align messaging and drive lead generation.
- Track sales metrics and forecast revenue to meet organizational goals.

Marketing
Scope: Branding, demand generation, and product positioning.

Responsibilities:

- Develop and execute marketing strategies to increase brand awareness and reach.
- Align marketing campaigns with product releases, sales objectives, and target market segments.
- Coordinate content creation, digital advertising, and social media engagement.
- Champion a consistent brand identity across all customer touchpoints.

Data

The company defines "Data" for the System to include:

- **TeamRetro Customer Data**
  - Retrospective data (ideas, reactions, groups, votes, comments)
  - Health check data (ratings, comments)
  - Team action items
  - Team agreements
  - Custom retrospective and health check templates
  - User account information (email addresses, names, avatars, password hashes)
  - SCIM groups and users
  - User requests (e.g., support or privacy inquiries)
- **Reports and Logs**
  - Activity logs (e.g., user actions, administrative events)
  - Admin logs
  - API logs
  - Error logs
  - Integration logs
  - System logs
- **Supporting Data**
  - Quotes, invoices, and contracts
  - Payment history
  - Customer queries, support tickets, and feature suggestions

The following table describes the personal information collected and processed as part of the System of GroupMap Technology. Reports can be viewed in the TeamRetro application and are downloadable in electronic Adobe Acrobat (PDF), Microsoft Excel (XLSX) or comma-delimited (CSV) value file formats. The availability of these reports is limited based on user role.

The following table describes the personal information collected and processed as part of the System of GroupMap:

Client Data	Reporting Options
Retrospective Data	Retrospective summary (PDF) Ideas report (CSV, XLSX) Ideas with comments report (CSV, XLSX) Actions report (CSV, XLSX) Retrospective activity report (CSV, XLSX) Team activity report (CSV, XLSX)
Health Check Data	Health check summary (PDF) Latest health report (CSV, XLSX) Historical health report (CSV, XLSX) Actions report (CSV, XLSX) Health check activity report (CSV, XLSX) Team activity report (CSV, XLSX)

Team	Teams report (CSV, XLSX) Team activity report (CSV, XLSX) Individual action report (CSV, XLSX)
Users	Users report (CSV, XLSX)

Privacy Commitments

Privacy Practices

GroupMap Technology is a Data Processor. GroupMap Technology collects and processes personal data as part of the System at the direction of the Data Controllers who are GroupMap Technology's customers who use the System. The data subjects, whose personal information is collected, are the Data Controllers' employees (and other invited team members and guests).

Personally identifiable information collected from Data Subjects include email address, full name, and internet protocol (IP) address. This information is collected through the online signup process, via invitation from an existing user, or via the optional SSO and SCIM integrations.

GroupMap Technology is committed to safeguarding personal information in accordance with relevant privacy laws and the TeamRetro Privacy Policy. Below are the key practices:

Privacy Policy and Consent

- Policy Presentation – Data subjects and Data Controllers are shown the TeamRetro Privacy Policy and Terms of Service upon account creation or invitation acceptance.
- Policy Coverage – The Privacy Policy explains how personal data and intellectual property are collected, used, retained, disclosed, and anonymized.
- Contact Information – The Privacy Policy identifies the assigned Privacy Officer, UK and EU Representative, along with the primary privacy@teamretro.com email address for inquiries.

Collection of Personal Information

- Personal Data: TeamRetro collects the user's email address, full name, and IP address for account setup and basic functionality. Additional optional details (e.g., avatars, language preferences) may also be stored.
- User-Generated Content: If individuals choose to include personal information in retrospectives or health checks, it remains visible only to authorized participants. TeamRetro never sells or monetizes this data.

Requesting Data Deletion or Export

- User Rights: Data subjects can request account deletion or personal data export by contacting privacy@teamretro.com or via in-app settings.
- Response Time: Requests are addressed within legally required timelines and in accordance with the TeamRetro Privacy Policy.

Data Usage and Sharing

- Purpose Limitation: Personal data is used solely for providing and improving the System (e.g., facilitating retrospectives, health checks, analytics, and troubleshooting).
- No Third-Party Advertising: TeamRetro does not use or share personal data for advertising or third-party analytics cookies.
- Authorized Sub-Processors: Certain third parties (e.g., hosting providers, payment processors) operate under Data Protection Agreements that align with TeamRetro's privacy, security, and confidentiality commitments.
- Compliance with Law: TeamRetro may disclose data if required by law, or if necessary to protect rights, property, or safety.

Security Measures

- Encryption: All data in transit uses SSL/TLS. Sensitive data at rest (e.g., password hashes) is protected by strong cryptographic methods.
- Hosting: The System is hosted by Amazon Web Services (AWS) with robust physical and environmental controls.
- Administrative Controls: Access is restricted on a least-privilege basis, with continuous monitoring for potential security events.

GroupMap Technology is committed to attestation reporting for the SOC 2 Trust Services Criteria related to Privacy to demonstrate the governance, accountability and alignment of its privacy commitments.

Sub-Processors

GroupMap Technology relies on a select group of specialized sub-processors to support the System's functionality, uptime and processing of personal data. Each sub-processor operates under a written agreement that enforces data protection and security obligations:

System	Type	Purpose
AWS	Infrastructure, storage cloud hosting	Cloud infrastructure for storing, processing and managing company and personal data.
DataDog	Infrastructure dashboards	Operational insights and alerts These monitoring and observability platforms are used exclusively for operational, performance, and security monitoring. They do not store or process personal data for advertising or third-party analytics purposes, in alignment with GroupMap Technology's 'no third-party analytics cookies' commitment.
BetterStack	Logging (BetterLogs)	
	Monitoring (BetterUptime)	
GitHub	Source code management, CI/CD, deployment pipeline	Change release testing through production deployment
Ably	Scalable web socket broadcasting	Real-time web socket-based data synchronization
SendGrid	Email delivery	Transactional and marketing emails
PayPal	Payment Gateway (Braintree)	Online subscription payments

Data Handling and Sub-Processor Oversight

Sub-processors comply with GroupMap's Privacy Policy, ensuring personal data is processed strictly for operational and service-related purposes. All third-party providers sign data protection agreements aligning with high security, confidentiality, and privacy standards. No sub-processor is permitted to use personal data for advertising, profiling, or resale.

In addition, GroupMap's responsibilities for handling sub-processors include:

- **Security Review:** Evaluating the vendor's documented security posture, including any available certifications or penetration test results.
- **Contractual Protections:** Ensuring the vendor signs a data protection agreement and commits to using data solely for agreed-upon operational purposes.
- **Annual Vendor Review**: The company classifies vendors based on risk profile. High-risk vendors undergo an in-depth annual review, during which the company re-validates security controls, certifications, and alignment with its compliance obligations.
- **Risk Register Updates**: Any new findings or changes in vendor risk status are recorded in a centralized risk register to ensure visibility and timely remediation if necessary.
- **Security Controls:** The company applies rigorous access control, encryption, logging, and monitoring to safeguard data both in transit and at rest.
- **No Advertising Use:** In accordance with the GroupMap Technology Privacy Policy, sub-processors are prohibited from using personal or customer data for advertising or third-party analytics.

Processes, Policies and Procedures

Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with GroupMap Technology's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all GroupMap Technology's employees and can be referred to as needed.

Physical Security

The critical infrastructure and data of the System are hosted by AWS. There are no trusted local office networks. As such, AWS is responsible for the key physical security controls that support the System. AWS holds multiple certifications (e.g., ISO 27001, SOC 1 and SOC 2, PCI Level 1) that validate the design and operating effectiveness of its physical security controls.

Since AWS provides Infrastructure-as-a-Service (IaaS), GroupMap Technology relies on AWS for data center environmental controls such as fire suppression, uninterruptible power supplies (UPS), and secure access control systems.

Logical Access

User Access Review
GroupMap Technology's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access management processes are followed to ensure access rights are reviewed annually and adjusted when no longer required. Additional information security policies and procedures require GroupMap Technology employees to use the systems and data in an appropriate and authorized manner.

Network Security
Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, monthly testing for and remediation of technical vulnerabilities, and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

Endpoint Device Management
GroupMap Technology employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data. Hexanode mobile device management software is used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

Role-Based Access Control (RBAC)
GroupMap Technology implements a role-based security architecture. Each user must be identified and authenticated before accessing any system resources. Access rights are provisioned based on a "least privilege" principle, tied to job responsibilities. Google Workspace authentication software is used for identity management and single sign on.

Multi-Factor Authentication (MFA)
All employees and contractors are required to use MFA for critical systems (e.g., AWS, GitHub, production servers). Passwords alone are insufficient for production access.

Google Workspace Single Sign-On (SSO)
Internal corporate systems, including Google Workspace, enforce password complexity and expiration settings. Employees log in via Google Workspace credentials or other approved SSO solutions. Systems not covered by Google Workspace have separate authentication that meets or exceeds the corporate password policy.

Onboarding and Termination

- Onboarding: New hires undergo a documented process that includes background checks (where legally permissible), assignment of roles, and approval of access.
- Role Change: When an employee's role changes, access is reviewed and adjusted appropriately.
- Offboarding: Upon termination, accounts are disabled immediately, and access roles are removed. The security team documents these changes in the access management system.

Session Lock and Timeout

Employee devices must auto-lock after 15 minutes of inactivity, in accordance with the Information Security Policy.

System Operations

System Monitoring

The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

Daily Encrypted Backups

Data of the System is automatically backed up on a daily basis via AWS Backup. All backups are encrypted at rest. Backup jobs are monitored for completion and any exceptions are immediately investigated.

Retention Period

Encrypted backups are retained for up to 30 days for disaster recovery purposes. Production data associated with cancelled accounts is retained for up to 365 days (or as otherwise agreed) in accordance with the TeamRetro Terms of Service and Privacy Policy.

Recovery Testing

Backup and restoration procedures for the System are defined and followed. Backup and recovery procedures are tested annually to verify that data can be successfully restored within required time frames.

Incident Management Policy

A formal Incident Management Policy outlines how to detect, classify, and respond to incidents, including security, privacy, or any suspected data breach. Incidents must be reported promptly to security@groupmap.com.

Incident Severity Levels

Incidents are categorized based on factors such as number of users affected, potential legal or contractual violations, and confirmed data breaches. Each category has specific escalation procedures and communication requirements.

Post-Incident Review

A post-incident review is conducted within 72 hours of resolution to identify root causes and corrective actions. This review process helps drive continual improvement.

Disaster Recovery and Business Continuity Plans

- Redundant Infrastructure: Critical components run in multiple AWS Availability Zones.
- Plan Testing: The disaster recovery plan and business continuity plan are tested annually, with outcomes documented and updates made as necessary.
- Capacity Monitoring: Resource usage such as CPU, memory and network use, are continuously monitored to ensure consistent performance and availability.

Change Control

Documented Software Development Life Cycle (SDLC)

GroupMap Technology operates a defined process for software development with supporting policies and procedures. GroupMap Technology follows a documented SDLC policy with a structured change management process.

Ticketing System
All changes—whether new features, bug fixes, or infrastructure updates—are logged and prioritized for development in a ticketing system. Each ticket includes details on the scope of work, associated risks, and testing requirements to support GroupMap Technology's System and objectives.

Peer Review
Code changes undergo peer review before merging into main branches. Developers review each other's commits, focusing on potential security, privacy, or performance issues.

Environment Separation
Changes are first deployed to a development environment for initial testing, then promoted to staging for final validation. Only after successful staging verification and managerial approval are changes promoted to production. This multi-environment approach reduces the risk of introducing defects into live systems.

Approvals and Signoffs
Major or high-risk changes require additional signoffs from the product owner or security lead. This ensures alignment with organizational objectives, including security and compliance standards.

Automated Testing and CI/CD
GroupMap Technology employs continuous integration and continuous deployment (CI/CD) pipelines that automatically run unit tests, static code analysis, and integration tests to catch issues early in the development cycle.

Version Control
GitHub version control software is used for the code repository that tracks all changes to the GroupMap Technology infrastructure, including managing versions and roll-back capability in the event of a failed change release.

Data Governance

GroupMap Technology uses data to support the System objectives and services. An approach to effective data governance has been established to understand and communicate the data that's used in the System, the objectives and requirements of that data, and the commitments of GroupMap Technology.

Established processes, policies, and procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

Encryption in Transit
All data transmitted between user browsers and the System is encrypted using SSL/TLS. This prevents interception or tampering by unauthorized parties.

Firewalls and Network Segmentation
AWS infrastructure includes layered firewalls, Virtual Private Clouds (VPCs), and network access controls. Unapproved traffic is denied by default.

Boundaries of the System

The scope of this report includes the GroupMap Technology TeamRetro Software as a Service System. This report does not cover the cloud hosting services provided by Amazon Web Services.

Changes to the System in the Last 12 Months

TeamRetro migrated its web socket broadcast functionality from Pusher to Ably to provide more robust real-time data synchronization.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Criteria Not Applicable to the System

All Common Criteria/Security, Availability, Confidentiality and Privacy Trust Services Criteria were applicable to GroupMap Technology's System.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

This report does not include the cloud hosting services provided by Amazon Web Services ('AWS').

Subservice Description of Services

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, Japan, and Australia AWS accreditations include ISO 27001, ISO 27017, ISO 27018, SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II), PCI Level 1, FISMA Moderate and Sarbanes-Oxley (SOX).

Complementary Subservice Organization Controls

GroupMap Technology's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the Agreed Criteria related to GroupMap Technology's services to be solely achieved by GroupMap Technology control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of GroupMap Technology.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Agreed Criteria described within this report are met.

Subservice Organization – <Name>		
Category	Criteria	Control
Common Criteria/ Security	CC6.1-CC6.8	Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
Common Criteria/ Security	CC6.4	Policies and procedures are established and followed to restrict physical access to data center facilities, backup media, and other system components, including firewalls, routers, and servers.
Common Criteria/ Security	CC7.1-CC7.5	Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to and resolve adverse events.
Common Criteria/ Security	CC8.1	Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested and approved prior to deployment into production.
Availability	A1.2	Procedures are established and followed to manage environmental protections within the data centers that house network, virtualization management, and storage devices supporting cloud hosting services where the system resides.

GroupMap Technology management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts, such as service level agreements. In addition, GroupMap Technology performs monitoring of the subservice organization controls including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Monitoring external communications, such as customer complaints relevant to the services provided by the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

GroupMap Technology's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Agreed Criteria related to GroupMap Technology's services to be solely achieved by GroupMap Technology control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of GroupMap Technology's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Agreed Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

User entities are responsible for:

- Understanding and complying with their contractual obligations to GroupMap Technology. In the event of a security incident affecting their system account, the user entity should report incidents immediately to security@groupmap.com.
- Notifying GroupMap Technology of changes made to technical or administrative contact information.
- Ensuring system user login additions and changes are authorized prior to being enacted.
- Ensuring system user logins are removed in a timely manner upon termination.
- Reviewing system user logins on a periodic basis to ensure access is restricted to authorized and appropriate individuals.
- Ensuring privileged roles on their system account, administrator and owner roles, are approved by appropriate personnel prior to being enacted.
- Ensuring the supervision, management, and control of the use of the system by the user entity's personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize the system.
- immediately notifying GroupMap Technology of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

Data controller responsibilities:

- User entities are responsible for obtaining consent from data subjects prior to the collection or processing of any personal data.
- User entities are responsible for having a privacy policy to notify data subjects of the requirements for consent, the choices available to data subjects and their rights in relation to the personal data.
- User entities are responsible for providing notice to their data subjects about its privacy practices to meet the user entity's objectives related to privacy.
- User entities are responsible for ensuring that personal information is collected consistent with the user entity's objectives related to privacy.
- User entities are responsible for communicating choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice.
- User entities are responsible for granting identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, providing physical or electronic copies of that information to data subjects to meet the user entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the user entity's objectives related to privacy.
- User entities are responsible for correcting, amending, or appending personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the user entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the user entity's

objectives related to privacy.

- User entities are responsible for disclosing personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the user entity's objectives related to privacy.
- User entities are responsible for obtaining commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the user entity's objectives related to privacy.
- User entities are responsible for providing notification of breaches and incidents to affected data subjects, regulators, and others to meet the user entity's objectives related to privacy.
- User entities are responsible for providing data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the user entity's objectives related to privacy.
- User entities are responsible for providing data subjects with means of contacting the entity with inquiries, complaints, and disputes regarding personal information.

Office Locations

AUSTRALIA
Level 3/11 York Street
Sydney NSW 2000

UNITED STATES
1400 Lavaca Street, Suite 700
Austin, Texas 78701

EMEA
Block 2 Charlemont Street, Charlemont Row
Saint Kevin’s, Dublin, D01 F6X6