TERAPAGE SECURITY & PRIVACY DOCUMENT

www.terapage.ai

Document Overview

This document outlines the technical and organizational measures (TOMs) implemented by Terapage to ensure compliance with various data protection standards such as GDPR, HIPAA, PIPEDA, and CCPA. It provides a high-level overview of Terapage's security measures. More detailed information on these measures is available upon request. Terapage retains the right to revise these TOMs at any time without prior notice, provided such revisions do not significantly reduce or weaken the protection afforded to personal data processed by Terapage. In the unlikely event of a significant security reduction, Terapage will notify its customers promptly. This document undergoes annual review and approval by Terapage's Senior Management Team.

Governance

Terapage's management demonstrates a firm commitment to implementing robust policies, procedures, and technical and organizational measures to ensure that the processing of Personal Data complies with applicable Data Protection (DP) laws and upholds the rights of data subjects. As an ISO 27001 and ISO 9001 certified organization, Terapage establishes clearly defined Data Protection roles and responsibilities across the organization, reinforcing its dedication to excellence and compliance in data privacy and quality management.

About Terapage

Terapage help firms understand the trends and insights that matter to them, in the ways that matter to their respondents. We believe that great things happen when people really understand each other. That is why we offer an innovative way to research human needs, their behaviours, journeys, and personal experiences. Understand the humans behind the pie charts, the sentiments behind the analytics, the why behind the what, who, when and where. We help you experience what they feel at work, online, at home, and in store in a way that's not just innovative, but real, raw, rich, and very human.

Accountability

Data Protection Policy and Associated Documents: Terapage creates and maintains appropriate data protection policies, procedures, and Technical Organizational Measures (TOMs) concerning the processing of Personal Data.

Copyright © Terapage – www.terapage.ai

Training and Awareness: All Terapage employees and individual contractors involved in processing Personal Data receive comprehensive Data Protection and Data Security Training at least once a year.

Activity Logging: Terapage meticulously records day-to-day activities to ensure compliance with Data Protection Laws. The organization ensures that all pertinent activities are logged and managed, adhering to its policy of documenting significant Data Protection events.

Record of Processing Activities (ROPA): Terapage maintains a detailed Record of Processing Activities (ROPA) to fulfill the requirements of Article 30 of the GDPR.

Risk Management: Terapage maintains a risk register that identifies and addresses data protection risks within the organization.

Employment Policies and Measures: Terapage aligns with GDPR principles in its employee/consultant recruitment, selection, and screening policies and procedures. Provisions pertaining to the access and handling of Personal Data are clearly outlined in employees' contracts of employment.
All Terapage employees are required to sign confidentiality agreements upon commencing employment. Access to systems is promptly revoked upon termination of employment.

Internal and External Compliance Reviews: Terapage conducts annual internal compliance reviews to assess its data protection compliance efforts. Additionally, the organization may engage in external compliance reviews as necessary.

Software Requirements

Terapage operates as a web-based program that works with all smartphones and web browsers. Its adaptive design is compatible with diverse screen resolutions, so the users don’t need to install web browser extensions, native mobile applications, or desktop software. Current compatibility consists of the latest versions of widely used web browsers:

- Google Chrome, Microsoft Edge, Mozilla Firefox and Apple Safari
- Mobile Safari for Apple iOS devices
- Google Chrome for Android devices

Secure Cloud Hosting

Copyright © Terapage – www.terapage.ai

Terapage is hosted within the cloud infrastructure of **Amazon Web Services** (“AWS”). AWS provides a scalable cloud computing platform with remarkable reliability and availability. Hence, both Terapage and Amazon share security responsibilities.

AWS Security

AWS assumes the responsibility for the protection of its global infrastructure that runs all of the services offered within the AWS cloud. This infrastructure consists of the software, hardware, networking, and facilities that operate AWS services.
Safeguarding this infrastructure is of great importance to AWS. While their data centers cannot be physically visited, AWS provides various reports from third-party auditors who have certified their compliance with various computer security standards and regulations (for further information, visit http://aws.amazon.com/compliance).
The IT infrastructure provided by AWS is developed and managed following security best practices and a range of IT security standards, comprising:

- SOC 1/SSAE 16/ISAE 3402
- SOC 2
- SOC 3
- FISMA, DIACAP, FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

Network Security

Terapage sites are strategically deployed within AWS to optimize security using a diverse range of automated tools, managed services, and best practices. The main objective is to enhance availability while stopping any unauthorized access.

- Within AWS, Terapage operates within its own Virtual Private Cloud (“VPC”) and security group.
- Terapage servers have no public interfaces except HTTPS connections, which are channeled through redundant load balancers.
- Automatically, HTTP connections on port 80 are redirected to HTTPS on port 443, ensuring the encryption of all data in transit.
- Secure SSH connections are accessible only to system administrators, which require connections via an IP-restricted VPN link connecting Terapage offices and AWS.

Copyright © Terapage – www.terapage.ai

External Security Testing

An external security firm is responsible for routinely conducting manual penetration tests on Terapage. A recent test certificate can be provided upon request.

- Dynamic security penetration testing is done to check a potential hacker's perspective of the application. Moreover, it is also employed to detect problems related to the application's environment and configuration.
- The activities undertaken during a penetration test are listed below:
- A comprehensive "crawl" of all authenticated and unauthenticated application screens is conducted through diverse test accounts, using both active and passive scan modes by a commercial vulnerability scanner. Each crawl request is validated for false positives and corresponding responses are documented in a log file for each test account.
- Business critical application screens, components, and workflows are marked for a manual code walkthrough to detect possible security defects.
- When suitable, potential vulnerabilities are exploited for proof-of-concept and to check exploitability.
- Attempts at Privilege escalation are made along with the attempts to obtain access to vulnerable systems and services.
- Network penetration testing is carried out which consists of scanning and host identification, network information gathering, user enumeration, port/service enumeration, and more.
- Log files are parsed to identify the application inputs that are processed by each page including cookies, headers, GET/POST variables, and more.
- Application inputs are reviewed to identify the nature and intended use of each value.
- Every application input undergoes testing for input-related vulnerabilities (fuzzing) and is then evaluated to ensure sufficient protection against tampering and/or unauthorized disclosure.
- Each application screen is tested to make sure the accurate enforcement of required authentication and/or authorization requirements together with related business logic controls.
- Application servers undergo scanning to identify common vulnerabilities and/or insecure configurations.
- Any compiled client-side code is decompiled and tested for potential vulnerabilities.

Copyright © Terapage – www.terapage.ai

- Proof-of-concept exploits are performed, and relevant screenshots are captured to demonstrate vulnerabilities.
- Evaluating the application using a 120-point security checklist to ensure maximum performance.

The methodology for web application penetration testing can discover the following flaws:

- Injection flaws
- Authentication flaws
- Session management flaws
- Cross-site scripting flaws
- Direct object reference flaws
- Server misconfiguration flaws
- Insecure data caching flaws
- Insecure data transmission flaws
- Information disclosure flaws
- Weak SSL/TLS ciphers
- Authorization and function level authorization flaws
- Cross-site request forgery flaws
- Invalidated redirects and forwards
- Clickjacking flaws
- File upload/download flaws

Security Monitoring

Through proactive system monitoring, Terapage gets real-time monitoring of the health of its infrastructure.

- Intrusion detection systems (“IDS”) employ a threat detection service to constantly monitor for any malicious activity.
- An external monitoring service validates the response time and health of each load balancer and web server after every 30 seconds. When response time thresholds are surpassed, alerts are activated. There are various points of presence around the globe from where monitoring can be performed.
- Monitoring notifications are forwarded to on-call engineers. Various activities can activate notifications such as server health alerts, network intrusion attempts, performance issues, and other malicious activities. OpsGenie is used to initiate an auto-escalating set of notifications through email, SMS, and phone calls until system administrators acknowledge the issues.

Copyright © Terapage – www.terapage.ai

- Customer-initiated issue escalation is offered to activate an instant alert to on-call system administrators. Escalations are submitted through https://terapage.raiseaticket.com/support/#/newticket

Data Security

Every Terapage site has multiple features to optimize the security of the imported and collected data:

- **Encryption of data in transit** shields all transmitted data as it travels across the Internet through the Transport Layer Security (TLS) protocol version 1.2 or later
- **Encryption of data at rest** protects all stored data within AWS using the industry standard AES-256 encryption algorithm
- **User actions are logged** through study visit histories, web server logs, database logs, and offsite application event tracking.
- **Web application routing rules** prevent forced navigation attacks by making sure that only authorized users have access to dynamic resources.
- **Dynamic request throttling** reduces the effectiveness of brute force attacks by actively blocking excessive requests coming from a single source.
- **Automatic authentication** from trusted devices and email notifications are time-restricted and can be disabled.
- **Aggressive content filtering** of users-inputs prevents Cross-Site Scripting ("XSS") and other similar attacks.
- **Secure form tokens** prevent Cross-Site Request Forgery ("CSRF") by guaranteeing that end users cannot be deceived into performing unintended actions while currently authenticated.
- **Integrated anti-virus protection** service scans all binary files submitted by users during uploads and can alert administrators of infected uploads.
- **A model-driven architecture** protects business data by developing a single "gate" to proxy all requests to add, view, update, or delete data.
- **Proprietary database abstraction layer** stops SQL injection attacks that can cause data leakage or loss.

Copyright © Terapage – www.terapage.ai

Database Content

Terapage uses a combination of CasandraDB, SQL, XML and Amazon Relational Database Service (“RDS”), an extensively secure and managed version of the MySQL database. In addition to the managed security of RDS, database replication is configured to extend over various AWS regions.

All database instances are hardened and inaccessible beyond the private network established within its AWS region. Terapage initiates the necessary data schema and manages future schema modifications with no risk of manual interference.

Data Transfer Management

Terapage shares Personal Data with external parties solely for identified purposes and ensures all necessary transfer mechanisms are in place.

Supplier and Partner Management: Terapage integrates data protection measures into supplier and partner activities by:

- Addressing Article 28 of the GDPR requirements in Data Processing Agreements (DPAs) with all relevant suppliers.
- Assessing processors to ensure they have established sufficient safeguards for processing Personal Data.
- Specifically evaluating processors for the security of processing and physical storage location of Personal Data.
- Ensuring all processing activities are conducted under contract, with processor contracts evaluated to ensure adequate safeguards and service levels are in place as needed.

Transparency

Terapage provides concise statements to data subjects, ensuring they receive all necessary information regarding its processing activities.

- Data Privacy Statements: The organization upholds transparency requirements mandated by Data Protection Laws and communicates pertinent details about its processing activities to data subjects.
- Employee Data Protection Notice: Terapage meticulously records its processing activities concerning employee Personal Data within the Employee Data Protection Notice.

Change Management

Copyright © Terapage – www.terapage.ai

Terapage establishes and enforces a structured approach to managing data protection risks and changes.

- Data Protection by Design: Terapage integrates principles of Data Protection by Design into systems and enhancements from the outset of development, while also providing annual education on data protection and cybersecurity for software development, testing, and support teams.
- Terapage conducts Data Protection Impact Assessments (DPIAs) in situations where its processing activities are likely to pose a high risk to the rights and freedoms of data subjects. DPIAs are ideally conducted before commencing relevant processing activities and evaluate the potential impact of planned processing operations on the protection of Personal Data.

Security Management

The organization ensures the security of its systems used for processing Personal Data.

- Information Security and Related Policies: Terapage has documented its Information Security Policies, which can be provided upon request. Terapage maintains comprehensive security and privacy policies/documents, including:
    - IT and Infrastructure Security Policy
    - System and Network Security Policy
    - Incident/Breach Management Policy
    - Access Control Policy
    - Asset Control Policy
    - Asset Management Register (Template)
    - Breach Management Measures
    - Bring Your Own Device Policy
    - Business Continuity & Disaster Recovery Plans
    - Data Protection Impact Assessment (DPIA) Register (Template)
    - Data Protection Impact Assessment (DPIA)
    - Data Subject Access Request (DSAR)
    - Encryption Policy
    - Incident and Breach Management Policy
    - Incident Reporting Template
    - IT and Infrastructure Security Policy
    - Physical Security Policy
    - Retention and Deletion of Data
    - Risk Register

Copyright © Terapage – www.terapage.ai

  - Record of Processing Activities (ROPA)
  - System & Network Security Policy
  - Data Classification Policy
  - PIPEDA Compliance
  - HIPPA Compliance
  - CCPA Compliance
  - GDPR Compliance
  - AI Transparency
  - Sustainability and Impact

- Business Continuity and Disaster Recovery Plans: Terapage has established and implemented appropriate measures for Business Continuity and Disaster Recovery concerning the processing of Personal Data.
- Backups: Terapage has established an adequate backup process to ensure the restoration of access to Personal Data in case of incidents, ensuring confidentiality, integrity, and availability of processed Personal Data.
- Retention and Deletion of Data: Terapage has implemented measures for managing retention time and executing subsequent actions such as anonymization or deletion when applicable.
- Network Security: Terapage employs network security infrastructure, including Firewalls, Intrusion Detection/Prevention Systems (IDS/IPS), and other security controls for continuous monitoring, restriction of unauthorized network traffic, and detection and mitigation of attacks. Security Measures include:
  - Patch Management
  - Anti-virus/Anti-malware
  - Threat Notification Advisories
  - Vulnerability Scanning (across all internal systems)
  - Annual Penetration Testing Process in place.

Binary File Content

Binary files uploaded to a Terapage site are kept on either Amazon Elastic File Store (“EFS”) or Amazon S3 and backed up within AWS.
Access to the binary files uploaded to a Terapage site requires an authenticated session, except in the condition of site assets required for the design of the site, such as a custom site logo.

Video and Audio Content

Copyright © Terapage – www.terapage.ai

Videos submissions within a Terapage site undergo secure processing to prepare them for playback and analysis, like extracting spoken words to generate timed-coded transcripts. Terapage offers two kinds of video submission: asynchronous (video uploads and webcam capture) and synchronous (live video meetings).
Asynchronous videos are converted to a consistent file format (MP4) by Amazon Elastic Transcoder and an extracted audio file is created for speech-to-text transcription by the Google Cloud Platform. All processing of asynchronous video content takes place in Europe unless the site is situated in the United States or Australia.
Irrespective of the video type, video processing partners are never given personal information and are not allowed to save video content for more than 60 days following the completion of processing.
When the completion of processing, videos are secured within encrypted Amazon S3 repositories and saved in the same place as the Terapage site where it was submitted. Video playback and downloads need an authenticated session and also make use of encryption during data transfer.

Deployment Options

Data Residency

Terapage utilizes the worldwide footprint of Amazon Web Services (AWS) by providing site deployments in any of five geographic areas:

- **Asia Pacific** (Seoul, Korea)
- **Asia Pacific** (Sydney, Australia)
- **Canada** (Montreal, Canada)
- **European Union** (Dublin, Ireland)
- **United States** (Northern Virginia, USA)
- **United Kingdom** (England, Northern Ireland and Wales)
- **Africa** (West and South)

This wide geographic distribution guarantees that Terapage has replicated its operations in various distinct AWS regions. All backups are arranged within AWS availability zones in the same region for achieving maximum resiliency.

Multi-Tenant Cluster

Copyright © Terapage – www.terapage.ai

Each region comprises a multi-tenant cluster which is an assortment of load balancers, web application servers, file storage services, and databases. Customers can choose a desired regional cluster or upgrade to a Dedicated Deployment.

Dedicated Deployments

A site can be organized as an exclusive instance of Terapage within any of the supported geographic areas. As an upgrade from the multi-tenant cluster, it contains dedicated load balancers, application servers, file stores, and database servers. Dedicated deployments can also be designed to utilize their own outgoing (SMTP) email server.

Copyright © Terapage – www.terapage.ai

TERAPAGE

Identity and Access Management

Terapage requires that all end users be authenticated to access a site. A site is made up of administrators (Analysts, Moderators, and Clients) that are allowed to oversee research participants.
Panelists are allocated to Segments and Studies which regulate their access to the site. Moderators and clients are administrative positions that must also be allowed access on a study-by-study basis. Administrators with client-role are basically study observers unless they are allowed additional consent.

The following are the key security features related to identity and access management:

- **Access control** is centrally administered via a Site Administration area that allows quick provisioning and de-provisioning of user accounts while retaining historic account access logs.
- **User roles** clearly define rights and permissions (Analyst, Moderator, Client and
- Panelist).
- **Two-factor authentication** (2FA) requires a one-time password from a second device with every login which results in a significant increase in security. Any user of the site can activate 2FA and its use can be mandated for entire user roles or specific individuals.
- **Sensitive account modifications** by end users, such as an alteration to their own username, email, or password, need secondary verification through email or 2FA.
- **Passwords are salted and hashed** before being stored in the database.
- **Password complexity rules** can be customized to meet prevailing customer standards.
- **Password expiry rules** can be implemented while preventing password re-use for a specific timeframe.
- **Emailed links** with special privileges, such as password reset links, expire automatically.
- **Automatic lockout** of accounts stops brute force attacks on account passwords. Administrators can customize the lockout sensitivity and duration of the lock period.
- **Session logs** verify each visited study and include the user's IP address, device information, browser version, and session time period.

Copyright © Terapage – www.terapage.ai

- **Sessions expiry limits** can be fixed individually for panelist and administrative roles. Users are automatically logged out at the end of their session.
- **Single sign-on integration** can be activated, as a premium choice, which can help control account creation and user authentication.

Session Management

Terapage customizes the display of each page to guarantee that only permitted content and features are presented to an end user.
Once an authenticated session has been started, a tracking cookie for the session is set in the web browser which permits the user to stay logged in between requests. The session duration can be configured individually for administrators and panelists.
Terapage generates a random 128-bit session ID which is managed by Apache Tomcat, a leading Web Server and Java Servlet container in the industry. The session ID is stored as a temporary session cookie by the Web browser. The cookie and session ID do not contain any identifying information. Session IDs are regenerated when a session expires and upon re-entry to the site and thus never used again.

Copyright © Terapage – www.terapage.ai

Secure Software Development

Application security starts with secure software development practices. Terapage uses an Agile development technique which ensures regular and consistent updates to the application.

Source Code Management

The software code base of Terapage is centrally managed in a private online code repository. Access to the source code is centrally managed and given to the development team only. All accounts are protected by 2-factor authentication.
Code modifications are submitted to one or more development branches. Branches separate streams of work, significantly highlighting and categorizing related changes in the source code. With time, each line of code can be credited to a developer, release, and development requirement.

Code Reviews

When development branches are ready to be integrated and verified in a staging environment, they are submitted for review. A request to merge code allows lead developers to examine code changes and offer feedback before integrating the code.
General feedback and comments related to the code are handled directly within the source code repository. Code merge requests will be approved only when all the identified developments have been implemented. Code changes are then integrated into a larger development branch closely associated with the Agile development cycle, called a Sprint.

Build & Test Automation

All code modifications in the main development branch result in the initiation of an automated software build process. Personalized build scripts are used to initiate unit tests and static code analysis tools. In case of failed compilations and failed tests, the build process stops automatically and sends a notification to the development team. Broken builds have high visibility because no further work can be done until build issues are resolved.

Pre-Production Environments

Pre-production staging servers offer the chance to analyze a Terapage development branch within a safe hosting space that mirrors the production environment of AWS. Multiple development branches can be deployed and verified at the same time which allows the quality assurance team to gain early access and better control.

Copyright © Terapage – www.terapage.ai

Code reviews and automated builds must be completed before development modifications are tagged as "ready to test." Any problems recognized during manual testing are checked with the primary work ticket and ultimately traced back to the original developer and their code modifications. A state of "Done" is withheld until the work is fully done with all issues resolved and re-testing is performed.

Deployment Automation

When a code package receives its approval for release, packaging, and deployments are handled by CI/CD pipelines. Multiple services support the automatic scaling, health monitoring of applications, and load balancing.

The status of the Terapage application is determined by health metrics and other aspects gathered by AWS.

Amazon CloudWatch provides monitoring dashboards for analysis of crucial performance metrics, like latency, CPU utilization, and response codes. CloudWatch alarms send notifications when metrics surpass critical thresholds.

Other external monitoring services are also used to track overall uptime and the existing validity of all SSL certificates used by customer sites.

Copyright © Terapage – www.terapage.ai

Privacy

Terapage provides support to thousands of customers in many countries. Our customers trust the application with great amounts of personal data and information from diverse industries, such as insurance, financial services, government, healthcare, and technology.

Privacy by Design

Crucial features related to privacy have been integrated into Terapage. For instance, Terapage studies can be conducted anonymously without impacting the user experience.

Privacy by Default

Terapage studies are organized to share only usernames with participants of a research study. The extent of personal data shared can be increased or decreased according to requirements. Each report, transcript, and data export utility enable the possibility to anonymise the data for long-term storage and sharing.

Obtaining Informed Consent

Most of countries need informed consent before collecting and processing private data. Consent statements must be clear, comprehensible and should give complete information on the processing of the user's private data. Terapage offers an extensive Agreements feature to assist customers in obtaining and tracking this informed consent from panelists before they take part in a research study.

Identifying Personal Data

Terapage permits personalized profile fields to be recognized as potentially containing personally identifiable information (PII). Such field-level identification makes sure that personal data can be selectively erased by using data anonymization features.

Minimizing Personal Data

Terapage need minimal user identification to operate effectively. Studies can be conducted without disclosing the identities of participants. Moreover, Single sign-on (SSO) integration is also available which helps in storing and managing private data outside the platform.

Personal Data Removal

Terapage permits the targeted removal of personally identifiable information (PII) while maintaining research contributions.

In a process that anonymizes response data, Terapage also grants control over the elimination of photos and videos submitted by users. It is possible to delete the photos while retaining the photo

Copyright © Terapage – www.terapage.ai

comments and captions. Similarly, Videos can be eliminated while retaining the extracted text and audio transcripts.

Full Data Removal

After the ending of a Terapage site subscription, all database and file data for that site becomes inaccessible to its end users.
The data for a closed site is kept and incorporated in an ongoing backup process for a duration of 120 days after the subscription period ends (“Retention Period”).
After the end of the Retention Period, the site data is permanently removed but may be kept in backups for an additional 90 days. After the permanent removal, it is impossible to recover a site's data.

GDPR

Terapage actively assists its customers in ensuring compliance with Canadian and European data protection regulations, including those provided in the **General Data Protection Regulation** (“GDPR”), which replaced the EU Data Protection Directive (also referred to as “Directive 95/46/ EC “) and became applicable on **May 25, 2018**.
If an organization gathers, transfers, hosts, or analyzes the private data of EU citizens, GDPR obliges the organization to use third-party data processors who assures their capability to justify the technical and organizational requirements of the GDPR.

Data Processing Agreement

Terapage provides the customers with a Data Processing Agreement (“DPA”), which governs the relationship between the Terapage (acting as a data processor) and the customer (acting as a data controller). The DPA assists the customer’s compliance with their responsibilities under EU data protection law.
Contractual commitments of Terapage ensure that customers can:

- Respond to requests from data subjects to correct, modify or remove private data.
- Be informed about and report personal data breaches to related supervisory authorities and data subjects according to GDPR timeframes.
- Show adherence to the GDPR regarding Terapage’s Services.

Copyright © Terapage – www.terapage.ai

Third-Party Sub-Processors

Currently, Terapage employs third-party sub-processors to offer some infrastructure services like email notifications and secure application hosting. Terapage uses a commercially reasonable selection procedure by which it assesses the security, privacy, and confidentiality practices of potential sub-processors that may have access to private data for short time periods.
Terapage obliges its sub-processors to fulfill all the obligations as those demanded by Terapage (as a Data Processor) as defined in Terapage's DPA.

Sub-Processor List

The following is the list of sub-processors that Terapage uses to host or process customer data:

- Amazon Web Services (Hosting infrastructure)
- Google Cloud Platform (Speech-to-text transcription)
- Agora (Recorded webcam video and screen recordings)
- Odoo (Sales orders, billing, and customer support)
- Open AI (AI text summary and analysis)
- Signable (For signing contracts and service agreements)

Data Breach Notification

Following are the numerous key steps that will be taken if the unexpected event of data breach happens:

- Any instant action needed to safeguard affected sites and their data such as restricting access or resetting all user passwords.
- A thorough analysis of log files created by intrusion detection devices, VPN access points, web servers, application servers, operating systems, and databases to evaluate the effect of any reported incident.
- Sending formal notification to affected end-users within 24 hours of the data breach detection.

Conclusion

The success of Terapage depends on delivering a consistent and secure service that follows regional privacy legislation. Our goal is to be an integrated and indispensable partner to our customers. If you want to know more about our security and privacy practices, please contact us for further information.

Copyright © Terapage – www.terapage.ai