Telepath Data Information Security Overview

Our Company and Product

Telepath Data is a Data and Artificial Intelligence company. Seventh Sense is our flagship SaaS product, which enables marketers to leverage their existing campaign and corporate email data to improve a variety of business outcomes. Seventh Sense mines your existing engagement data to build profiles on every person that has engaged with your company and automatically discovers the ideal time and frequency to contact each individual.

Once profiles are built, Seventh Sense provides a suite of tools that make it make it simple to for you to take advantage of their insight; you can access the raw information via our API; you can integrate the information in your CRM and email systems; and you can automatically deliver your campaigns to each individual at their top engagement time and with optimized frequency.

Security and Risk Governance

Our primary security focus is to safeguard our customers' and users' data. In order to do that, we maintain an active information security management system based on the framework outlined in the ISO 27001 standard. As a result of the ongoing process of risk analysis and mediation, information security policies are mandated and approved by the company management. These policies drive selection of new controls, refinement of existing controls, and ongoing assessments of control efficacy. The security program is managed by our Chief Security Officer, who is a member of the Executive Committee and reports to the CEO.

Security and Risk Management Objectives

Our security framework has been developed to ensure we meet the following objectives:

- Customer Trust and Protection – consistently deliver superior product and service to our customers while protecting the privacy and confidentiality of their information.
- Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized individuals and proactively minimize the security risks threatening service continuity.
- Information and Service Integrity – ensure that customer information is never corrupted or altered inappropriately.
- Compliance with Standards – implement process and controls to align with current international regulatory and industry best practice guidance. We have designed our security program around best-of-breed guidelines for cloud security. In particular, we leverage standards like Cloud Security Alliance CCM, and align our practices with ISO 27001 and NIST SP 800-53.

Product Infrastructure

Data Center Security

We outsource hosting of our product infrastructure to leading cloud infrastructure providers. Principally, we leverage Amazon Web Services (AWS), which provides industry leading levels of physical and network security. At present, our AWS cloud server instances reside in US locations. Facilities uptime is guaranteed between 99.95% and 100%, and the facilities ensure a minimum of N+1 redundancy to all

power, network, and HVAC services. Access to these sites is highly restricted to both physical access as well as electronic access through public (internet) and private (intranet) networks in order to eliminate any unwanted interruptions in our service to our customers. The physical, environmental, and infrastructure security protections, including continuity and recovery plans, have been independently validated as part of their SOC 2 Type II and ISO 27001 certifications. Certificates are available at the AWS compliance site.

Network Security & Perimeter Protection

Our product infrastructure is built with internet-scale security protections in mind. In particular, network security protections are designed to prevent unauthorized network access to and within the internal product infrastructure. These security controls include enterprise-grade routing and network access control lists (firewalling).

Network-level access control lists are implemented in AWS Virtual Private Cloud (VPC) security groups, which apply port- and address-level protections to each of the server instances in the infrastructure. This allows for finely grained control for network traffic from a public network as well as between server instances on the interior of the infrastructure. Within the infrastructure, internal network restrictions allow a many-tiered approach to ensuring only the appropriate types of devices can communicate. Changes in the network security model are actively monitored, and controlled by standard change control processes. All existing rules and changes are evaluated for security risk, and captured appropriately.

Application Security

Web Application Firewall

As part of our commitment to protecting customer data and websites, we have implemented a Web Application Firewall (WAF) protecting our system (and your data) from Distributed Denial of Service (DDoS) and other web application attacks. The WAF is configured with a combination of industry standard and custom rules that are capable of automatically enabling and disabling appropriate controls to best protect our customers. These tools actively monitor real-time traffic at the application layer with ability to alert or deny malicious actors based on behavior type and rate.

Development and Release Management

Telepath Data provides constantly improving products through a modern continuous delivery approach to software development. New code is proposed, approved, merged and deployed daily. Approval is controlled by designated repository owners. Once approved, code is automatically submitted to a continuous integration environment where compilation, packaging and unit testing occur. If all tests pass, the new code is deployed automatically across the staging application tier. All code deployments create archives of existing production-grade code in case failures are detected by post-deploy hooks. Based on customer needs and in-person testing on the staging server, updates are deployed to the production system via rolling releases, ensuring continuous service.

Customer Data Protection

Architecture and Data Segregation

Telepath Data services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific unique identifiers and allows the use of customer and user role based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the "Infrastructure and Sub-processors" documentation available at https://www.theseventhsense.com/trust.

Control of Processing

Telepath Data has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Telepath Data and its sub- processors. In particular, Telepath Data has entered into written agreements with their sub-processors containing privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities. Compliance with such obligations as well as the technical and organizational data security measures implemented by Telepath Data and its sub-processors are subject to regular audits. The "Infrastructure and Sub-processors" documentation describes the sub- processors and certain other entities material to Telepath Data provision of the Services.

Sensitive Information

All information collected in our products is provided by our customers, either directly via our API, or indirectly by connecting to data sources such as marketing automation or email systems. Per the Telepath Data Terms of Service, our customers ensure that Telepath Data products are not used to collect or capture sensitive data such as credit or debit card numbers, personal financial account information, Social Security numbers, passport numbers, driver's license numbers or similar identifiers, or employment, financial or health information.

Credit Card Information Protection

Many Telepath Data customers pay for the service by credit card. Telepath Data does not store, process or collect credit card information submitted to us by customers. We leverage trusted and PCI-compliant payment vendors to ensure that customers' credit card information is processed securely and according to appropriate regulation.

Encryption In-Transit & At-Rest

All customer interactions with Telepath Data products (e.g., API calls, login, authenticated user sessions, etc.) are encrypted in-transit using TLS configured with best-practice key exchange protocols and ciphers in accordance with our Cryptography Policy. Telepath Data leverages several technologies to ensure stored data is encrypted at rest. Long-term storage solutions and databases are encrypted using best practice key management and ciphers in accordance with our Cryptography policy. The Telepath Data Cryptography Policy (and encryption controls based on it) is updated regularly based on industry best practice recommendations from sources including Amazon Web Services, Cloudflare, SANS and CERT.

User Authentication & Authorization

Telepath Data products leverage a bulk-heading approach to user authentication, authorization and management by leveraging a third-party authentication service. By leveraging this service, Telepath Data Users are protected by a robust set of password complexity controls, multi-factor authentication, social and enterprise single-sign on. In addition to password complexity requirements, the system automatically detects compromised passwords and proactively requires the user to reset their credentials before the account can be compromise. Application programming interface (API) access is

enabled through either API key or OAuth 2. Customers have the ability to generate API keys via their account settings user interface. Authorization for OAuth-enabled requests is established through defined scopes, which must be approved by an authorized user.

Employee Access

Telepath Data controls individual access to data within its production and corporate environment. A subset of Telepath Data's employees are granted access to production data based on their role in the company through role based access controls (RBAC). Engineers and members of Operations teams may be granted access to various production systems, as a function of their role. Common access needs include alert responses and troubleshooting, as well as to analyze information for product investment decisions as well as product support. Access to the product infrastructure is limited by network access and user authentication and authorization controls. Access to networking functions is strictly limited to individuals whose jobs require that access, and access is reviewed on a continual basis. Customer Support, Services, and other customer engagement staff with a need-to-know may access to customer accounts in conjunction with their work responsibilities associated with supporting and servicing our customers. All access requests, logins, queries, page views and similar information are logged.

Privacy

The privacy of our customers' data is one of Telepath Data's primary considerations. As described in our Privacy Notice, we never sell your Personal data to any third parties. The protections described in this document and other protections that we have been implemented are designed to ensure that your data stays private and unaltered. Telepath Data products are designed and built with customer needs and privacy considerations in the forefront. Our privacy program incorporates best practices, customers' and their contacts' needs, as well as regulatory requirements including but limited to the EU General Data Protection Regulation (GDPR). Customers may access the GDPR specific documentation, including the Telepath Data Data Processing Addendum at https://www.theseventhsense.com/trust.

Data Retention

Customer data is retained for as long as you remain a customer. Former customers' data is removed from live databases upon a customer's written request or 90 days after all customer relationships are terminated. Information stored in replicas, snapshots, and backups is not actively purged but instead naturally ages itself from the repositories as the data lifecycle occurs. Telepath Data reserves the right to alter the data pruning period and process at its discretion in order to address technical, compliance, or statutory needs.

Business Continuity & Disaster Recovery

Telepath Data maintains business continuity and disaster recovery plans focusing both on preventing outage through redundancy of telecommunications, systems and business operations, and on rapid recovery strategies in the event of an availability or performance issue. Whenever customer-impacting situations occur, Telepath Data's goal is to quickly and transparently isolate and address the issue.

System Resiliency & Recovery

Business continuity testing is part of Telepath Data normal processing. Telepath Data recovery processes are validated continuously through normal maintenance and support processes. We follow continuous deployment principles and create or destroy many server instances as part of our regular daily maintenance and growth. We also use those procedures to recover from impaired instances and other failures, allowing us to practice our recovery process every day.

Telepath Data primarily relies on infrastructure redundancy, real time replication and backups. All Telepath Data product services are built with full redundancy. Server infrastructure is strategically distributed across multiple distinct availability zones and virtual private cloud networks within our infrastructure providers, and all web, application, and database components are deployed with a minimum of n+1 supporting server instances or containers.

Backup Strategy

Telepath Data ensures data is replicated and backed up in multiple durable data-stores. The retention period of backups depends on the nature of the data. Data is also replicated across availability zones and infrastructure locations in order to provide fault-tolerance as well as scalability and responsive recovery, when necessary. In addition, the following policies have been implemented and enforced for data resilience:

- Customer (production) data is backed up leveraging multiple online replicas of data for immediate data protection. All production databases have no less than 1 primary (master) and 1 replica (slave) copy of the data live at any given point in time. A minimum of seven days' worth of backups are kept for any database in a way that ensures restoration can occur easily. Snapshots are taken and stored to a secondary service no less often than daily and where practicable, real time replication is used. All production data sets are stored on a distributed file storage facility like Amazon's S3.

- Because we leverage cloud services for hosting, backup and recovery, Telepath Data does not implement physical infrastructure or physical storage media within its products. Telepath Data does also not generally produce or use other kinds of hard copy media (e.g., paper, tape, etc.) as part of making our products available to our customers.
- By default, all backups will be protected through access control restrictions on Telepath Data product infrastructure networks, encryption at-rest per our Cryptography Policy, and access control lists on the systems storing the backup files.

Telepath Data Corporate Security

Employee Authentication & Authorization

Telepath Data enforces an industry-standard corporate password policy, which requires all passwords to meet a minimum entropy requirement. In most cases, and for all cases involving administrative access, multi-factor authentication is required in addition to a password. Wherever possible, single-sign on via our corporate G-Suite account (which requires multi-factor authentication) is used to authenticate to any third-party services. Telepath Data prohibits account and password sharing by multiple employees.

Background Checks

All Telepath Data employees undergo a background check prior to formal employment offers. Reference verification is performed at the hiring manager's discretion. All employees receive security training within the first month of employment as part of the Telepath Data security program along with role-specific follow-up training. All employees must comply with Non-Disclosure Agreements and Acceptable Use Policy as part of access to corporate and production networks.

Vendor Management

We leverages a small number of 3rd party service providers to deliver our services. In order to ensure these providers meet the standards we hold for ourselves, we maintain a vendor management program to ensure that appropriate security and privacy controls are in place. The program includes inventorying, tracking, and reviewing the security programs of the vendors who support Telepath Data. Appropriate safeguards are assessed relative to the service being provided and the type of data being

exchanged. Ongoing compliance with expected protections is managed as part of our contractual relationship with them.

Security Awareness & Security Policies

Multiple levels of security training are provided to Telepath Data employees, based on their roles and resulting access. General security awareness training is offered to all new employees and covers Telepath Data security requirements. To help keep all our engineering, support, and other employees on the same page with regard to protecting your data, Telepath Data developed and maintains a set formal Information Security Policies. The policies are updated (and approved) on a continuous cycle, and include the following:

- Information Security Policies
    - Risk Assessment Policy
- Human Resources Security
    - Acceptable Use Policy
    - Clean Desk Policy
    - Conduct and Ethics Policy
- Asset Management Policy
    - Information Classification Policy
- Access Control
- Cryptography
- Physical and Environment Security Policy
- Operational Security
    - Change Management Policy
    - Server Security Policy
    - Workstation Security Policy
    - Mobile Device Policy
    - Removable Media Policy
- Communications Security
    - Network Security Policy
- Systems Acquisition, Development and Maintenance
    - Application Security Policy
    - Secure Development Policy
    - Privacy Policy
- Supplier Relationships
    - Third Party Security Policy
- Incident Management Policy
    - Data Breach Response Policy
- Business Continuity Management
- Compliance

Incident Management

Telepath Data provides endeavors to respond quickly to all security and privacy events. Telepath Data's rapid incident response program is responsive and repeatable. Many automated processes feed into the incident response process, including malicious activity or anomaly alerts, vendor alerts, customer requests, privacy events, and others. In responding to any incident, we first determine the exposure of the information and determine the source of the security problem, if possible. We communicate back to the customer (and any other affected customers) via email or phone (if email is not sufficient). We provide periodic updates as needed to ensure appropriate resolution of the incident. Our Chief Security Officer reviews all security-related incidents, either suspected or proven, and we coordinate with affected customers using the most appropriate means, depending on the nature of the incident.

Product Security Features

Telepath Data’s security program is designed to protect all past, current and future Telepath Data products. Each product takes advantage of common application development security best practices as well as infrastructure security and high availability configurations.

Whether our products are free or paid, feature-rich or lightweight, Telepath Data works hard to maintain the privacy of data you entrust with us. Data you store in Telepath Data products is yours. We put our security program in place to protect it, and use it only to provide the Telepath Data service to you. We never share your data across customers and never sell it, although we do reserve the right to use our anonymous observations of your data to make further improvements to our products.

Gmail Integration

As a Seventh Sense user, you have the ability to connect your Gmail account to the system. Gmail integrations are authorized by and protected by the native integration capabilities provided by google including requiring you to grant access for each type of access needed. This access can be revoked at any time via your Gmail settings.

HubSpot Integration

As a Seventh Sense user, you have the ability to connect your HubSpot marketing portal to the system. HubSpot integrations are authorized by and protected by the native integration capabilities provided by HubSpot including requiring you to grant access for each type of access needed. You will need the

HubSpot super-admin role to initiate the connection. This access can be revoked at any time via your HubSpot portal.

Marketo Integration

As a Seventh Sense user, you have the ability to connect your Marketo marketing automation system to the system. Marketo integrations are authorized by and protected by the native integration capabilities provided by Marketo including requiring you to grant access for each type of access needed. Further documentation on the roles needed for the integration to function can be found in the Marketo Connector Setup guide. This access can be revoked at any time via your Marketo administration interface.

Third Party Audits And Certifications

Telepath Data services are housed in the US with world-class cloud infrastructure providers; Amazon Web Services and Google Cloud Platform. All Telepath Data infrastructure providers are SOC 2 Type II and ISO 27001 certified and maintain facilities secured against electronic and physical intrusion.

Document Scope and Use

Telepath Data values transparency in the ways we provide solutions to our customers. This document is designed with that transparency in mind. We are continuously improving the protections that have been implemented and, along those lines, the information and data in this document (including any related communications) are not intended to create a binding or contractual obligation between Telepath Data and any parties, or to amend, alter or revise any existing agreements between the parties.