Latitude Network Privacy & Data Management Policy

This policy focuses on data we manage and analyse on behalf of our clients

Information we receive - de-identified data

Latitude Network Pty Ltd consults with and provides data analytics services to a range of clients in the social services including not-for-profit organisations and government agencies. Information we collect, store and analyse on behalf of our clients is always de-identified information. That means **we do not have the means to identify an individual** from the data we manage - there are no names, addresses, phone numbers or email addresses contained in the data. Usually the data contains unique identifiers (random numbers that 'stand in' for an individual) that are not linked to identifiable information. We use controls and safeguards in the data access and storage environment to prevent identification or re-identification of data. The data we receive may also contain information collected by our clients or their partners such as survey results, usage of services, activities delivered and demographic information (such as gender and age).

Why we collect it and how we use it

Our Clients usually collect the data through their own data management systems which are covered by their privacy and consent policies with their clients. Clients then upload de-identified data to us using secure servers that are based in Australia. Most data is stored in our secure Azure data warehouse. For some services we may automate ingestion of data from client systems via APIs or other credentials. We then collect and store that information on behalf of our clients to assist them to understand their data, what outcomes they are achieving and how to improve their performance. Our overall purpose in using data is limited to helping social service organisations and governments improve performance and achieve better social outcomes.

We never use any client's data to conduct marketing activity to their clients (the beneficiaries of the services). We don't receive, keep or use personal or contact data for the beneficiaries of client programs. We may share the aggregate analysis of data (e.g. averages for a group of people in dashboards or chart visualisations) with our clients with their permission, or in some cases high level data is shared with our client's partners when it is requested/approved. We may also generate datasets on behalf of our clients and use machine learning techniques to analyse that data in order to demonstrate outcomes, understand what services work for which cohorts, or how social organisations can better manage their services for highest impact. All of that analysis is private and confidential to our clients, and they can then choose how they use it within their privacy policies. We don't publish reports from our client work to public servers.

How we keep data secure

We keep data secure by a combination of secure technologies and best practices.

Any data provided by our clients is stored on servers located in Australia.

Data provided to us will be stored in encrypted disks ("encrypted at rest"). Any movement of data will also be encrypted ("encrypted in transit") and audit logs are maintained that track access to the data by users. This covers our central storage facility (from our service provider Microsoft), external processing services (e.g. machine learning platforms) and any electronic device used by our analysts when accessing or working with data.

Clients share data with us only via our secure folders and via authorised uploads to our Azure data warehouse. No data is received, sent or kept in unencrypted form (e.g. email) or physical form (e.g. removable or portable disks, printed media). Clients can't access the data from our servers once it is uploaded.

We follow a "need to know'' principle when it comes to data access. Our data analysts are granted access to client data only when it is necessary to conduct work. No anonymous access is allowed. We make use of commercially reasonable best practices and technologies to ensure this. See our System Security Measures outlined below.

Keeping data de-identified

We work with clients to ensure data shared with us is already de-identified. Where practicable, this includes removing or altering any attribute that may allow someone to re-identify an individual (such as user IDs from database systems). In addition to this, data generalisation and grouping takes place where data is expressed in summary form by grouping related values into categories or ranges.

In the case where data containing identifying information may be accidentally uploaded to our systems, we remove it immediately, notify our client and work with them to prevent any recurrences.

In long-term projects where granular data is not strictly necessary, we only keep aggregated information.

How we align to our clients data policies

We recognise our client's role as the main controller of the datasets they provide to us. We work with our clients to align to their data privacy policies where applicable.

Upon termination of a service agreement, data is deleted from our systems, unless retention is required by post-agreement obligations.

Our service agreements regulate how we govern data for each client in accordance with the policies outlined in this document.

Using our client platforms

From time to time, we use our clients' platforms and servers to conduct analysis on their behalf. In those cases, we fully abide by their data privacy policies managing and processing data on their facilities.

Data breaches

In the unlikely event that the data stored has been or has likely been the subject of misuse, interference, unauthorised access, modification (or loss), or unauthorised disclosure, we will notify our clients and work with them to assess the impacts and carry out mitigation actions. We maintain Cyber Insurance to cover legal advice, management and mitigation in the event of a data breach.

Applying the 'Five Safes' data confidentiality framework

Latitude Network adopts the principles in the 'Five Safes' data confidentiality framework, as promoted by Australian Governments.

1. **Safe People**
   a. Latitude Network restricts access to client data only to a single Director and data analysts working on that client project. No other Latitude Network staff have access to that client's data.

b. All staff sign client confidentiality agreements.

c. We include client confidentiality clauses in our contracts for service with clients.

2. **Safe Projects**

a. All data analysis is conducted under a proposal with our client that specifies the purpose of the project. This purpose is agreed with our client prior to starting a project and the client gets internal approvals and is responsible to ensure that the purpose aligns with the organisation’s mission and policies.

b. Latitude Network’s purpose with all use of client data is for a public benefit - to improve achievement of outcomes and increase the capability of organisations to deliver high performance social outcomes.

c. We only provide our reports to our clients. The data is not used for regulatory or compliance purposes and is not provided to any other individual or organisation unless requested by our client in writing.

3. Safe Settings

a. We use an Australian-based server architecture with a provider used by many health and government departments, compliant with Australian Government data security requirements.

b. Our system includes full version control, user access control, two-factor authentication, and full traceability of access.

c. We only receive client data via a secure upload to this server, never via email or other insecure platform.

4. Safe Data

a. In general, we receive data uploads on a periodic or one-off basis for specific datasets. We do not receive access to live client databases - when we build dashboards for clients those are implemented internally to the organisation using their security management protocols.

b. We group data at a granularity that obscures unit records; including aggregation of data as well as more advanced techniques.

c. We delete client data that is no longer needed for a client project at the end of that project.

d. We encourage our clients to adopt robust privacy policies and respectful data collection methods, and to provide easy access for their clients of their information.

5. **Safe Outputs**
    a. Our reports go direct to our clients and are not shared publicly (unless that is the purpose of the project). Most work is used by Executives, senior managers or team leaders of our clients and is confidential and kept within the organisation.
    b. Most reporting we do is at the aggregate level (e.g. organisation-wide or at a program level containing averages for many individual clients) and so is safe from re-identification.
    c. Access to dashboards or other reports is managed within our clients' data management policies and procedures using their existing systems. Our clients manage who gets access to particular dashboards or reports.
    d. When we run collaborative data projects we provide aggregated data and we de-identify the individual organisations that provide that data from the report.
    e. Where we share our work in public settings (e.g. on our website or presenting at conferences) we use 'dummy' data or obscured data to generate visualisations.

System Security Measures

We implement a range of system security measures to reduce the risk of unauthorised access to any data we hold on behalf of our clients. These include -

1. Network Security

Azure SQL Database: Utilize IP firewall rules, virtual network firewall rules, and network security groups (NSGs) to control access to databases and servers based on IP addresses and virtual network subnets.

Azure Storage Accounts: Implement Azure Virtual Network service endpoints, firewall rules, and NSGs to restrict access to storage accounts and manage inbound and outbound traffic.

2. Access Management:

Azure SQL Database: Implement role-based access control (RBAC) within Azure portal for managing access to databases and servers. Employ SQL authentication and Microsoft Entra ID authentication for user authentication.

Azure Storage Accounts: Enforce RBAC to manage access to storage resources. Define access policies and permissions to control data access.

3. Authorisation:

Azure SQL Database: Control access to resources and commands within databases by assigning permissions. Utilize row-level security for granular control over data access. Implement dynamic data masking to limit sensitive data exposure by masking it to non-privileged users.

Azure Storage Accounts: Enforce authorization controls within storage accounts by defining access policies and permissions. Utilize Shared Access Signatures (SAS) for limited access.

4. Security Management:

Azure SQL Database: Regularly review and audit access controls, permissions, and configurations for databases and servers. Conduct vulnerability assessments to identify and remediate security vulnerabilities.

Azure Storage Accounts: Conduct regular reviews and audits of access controls, permissions, and configurations for storage accounts. Implement security best practices such as data encryption and secure data transfer protocols.

Access to Azure Resources: Utilize Virtual Private Network (VPN) connections for secure access to Azure resources. Implement resource connectors and configure connections to establish secure communication between on-premises networks and Azure resources. Utilize Zero Network Trust principles facilitated by Twingate for strict access control and detailed usage reporting. Conduct regular security assessments and audits to ensure compliance with security standards and regulatory requirements.

5. Dynamic masking

Implement dynamic data masking in Azure SQL Database to limit sensitive data exposure, ensuring that Personally Identifiable Information (PII) is not retrieved during data ingestion where possible. In scenarios where the data source provides all information, data containing PII is treated as transient and not stored in any layers to maintain compliance with data privacy regulations.

Policy Updates

This Policy may change from time to time and is available on our website www.latitude.network.

Privacy Policy Complaints and Enquiries

If you have any queries or complaints about our Privacy Policy please contact us at info@latitude.network