Privacy Policy

Logical Solutions 2020 Limited

Version 1.4
Effective date: 11 November 2026
Last updated: 11 November 2026

1. About this policy

Logical Solutions 2020 Limited ("Logical Solutions", "we", "us", "our") is a managed IT services provider based in Hamilton, New Zealand.

This policy explains how we collect, use, store, disclose, retain and delete personal information in connection with:

- our website, sales and marketing activities;
- our managed IT services, including helpdesk, support, remote monitoring and management, and on-site services;
- our data centre and hosting services, including hosted servers, virtual machines, storage, backup and disaster recovery; and
- our Business Intelligence and Data Warehouse Platform, which consolidates data from a customer's business systems into a hosted repository so that the customer's authorised users can report on and query it.

We comply with the Privacy Act 2020 (New Zealand). Where we handle information that is subject to other privacy laws, we also comply with those laws to the extent they apply.

2. Key terms

Term	Meaning
Personal information	Information about an identifiable individual, as defined in the Privacy Act 2020 (NZ). Where other laws apply, it also carries the meaning of "personal data" under the UK/EU GDPR.
Customer	A business that engages Logical Solutions to provide managed IT, data centre and hosting, or Business Intelligence and Data Warehouse services.
Customer Data	Data belonging to or controlled by a Customer that is stored on, transmitted through or processed by systems we manage or host for that Customer. This may include personal information about the Customer's own staff, clients, suppliers and contacts.
BI Platform	Our Business Intelligence and Data Warehouse Platform, including any reporting, dashboard and AI-assisted query features.

3. Our role: controller and processor

Our role depends on the data:

- Where we act as the **controller** (a "collecting agency"): information we collect for our own purposes, including website enquiries, sales and account contacts, billing records, service tickets raised with us, and our own staff records. We decide how this information is used and we are directly accountable for it under this policy.
- Where we act as a **processor** (an "agent" of the Customer): Customer Data held on systems we manage or host for a Customer, or processed by the BI Platform. Here the Customer is the controller. We process that data only to provide the services the Customer has engaged us for, under a written services agreement, and we do not use it for our own purposes.

If we hold your information on behalf of one of our Customers, please direct requests about it to that Customer in the first instance. We will assist the Customer in responding.

4. Information we collect

4.1 Information you give us directly

Name, business name, job title, email address, phone number, the content of your enquiry, and any information you include in correspondence with our sales or support teams.

4.2 Information collected through our website

IP address, browser and device type, pages visited, referring URL, and approximate location derived from IP address. See Section 14 (Cookies).

4.3 Information collected in the course of providing managed IT services

Support tickets and call records, contact details of Customer staff, device and asset inventories, user account details we administer, system and security logs, configuration data, remote support session records, and diagnostic information from Customer environments.

4.4 Information held in our data centre and hosting services

Customer Data stored on servers, virtual machines, storage and backups we host. We do not generally access the content of this data; we access it only as described in Section 7. We also keep technical records needed to operate these services, such as system, network and access logs, and records of who has been granted physical or remote access to our facilities.

4.5 Customer Data ingested into the BI Platform

We ingest only the data sources a Customer instructs us to connect. Typical sources include:

- helpdesk and ticketing systems;
- document management and file repositories;
- accounting and finance systems (for example Xero);
- telephony platforms, including call detail records and, where enabled, call recordings and transcripts;
- email and calendar systems;
- CRM and quoting systems; and

- line-of-business applications specified during discovery.

The specific sources, fields and date ranges connected for each Customer are documented in that Customer's discovery documentation and services agreement. Customers are responsible for ensuring they have a lawful basis for providing this data to us and for notifying the individuals concerned.

4.6 Information generated by the BI Platform

User account and authentication records, queries submitted by authorised users, reports and AI-generated responses, references to the source records used to answer a query, timestamps, and audit logs of access and activity.

5. Sensitive information

We do not seek sensitive personal information — including health information, biometric or genetic data, government identifiers, financial account numbers, precise geolocation, racial or ethnic origin, religious or political beliefs, trade union membership, sexual orientation or sex life, or information about criminal convictions — for use in the BI Platform, and we instruct Customers not to send it to us unless it has been expressly scoped, documented and approved in writing as part of the service.

Customer systems we manage or host may contain sensitive information that belongs to the Customer. We handle it only as needed to provide the service and protect it in line with Section 12.

6. How we use information

We use personal information only for the following purposes:

1. to respond to enquiries and provide quotes, proposals and letters of intent;
2. to deliver, configure, monitor, support and maintain the managed IT services a Customer has engaged us to provide;
3. to host, operate, back up, restore and protect Customer systems and data in our data centres;
4. to ingest, transform, index and store Customer Data in the BI Platform, and to answer authorised users' reports and queries;
5. to secure our systems, investigate incidents, prevent fraud and abuse, and maintain audit trails;
6. to invoice and collect payment, and to maintain financial and tax records;
7. to send service notices and, where you have agreed or it is otherwise permitted by the Unsolicited Electronic Messages Act 2007, newsletters and information about our services. You can unsubscribe at any time; and
8. to meet our legal, regulatory and contractual obligations.

Where the GDPR applies, our lawful bases are: performance of a contract (purposes 1–4, 6), legitimate interests (purposes 1, 5, 7), legal obligation (purposes 6, 8) and, where required, consent. Where consent is the basis, it may be withdrawn at any time.

We do not sell personal information, and we do not share personal information for advertising purposes.

7. Data centre and hosting services

Where data is hosted. Customer systems and data hosted by us are stored on infrastructure we operate in New Zealand data centres, unless a Customer has agreed otherwise in writing.

Customer control. The Customer remains the owner and controller of its hosted data. We do not use hosted Customer Data for our own purposes, and we do not sell, rent or share it.

When we access hosted data. Our engineers may access hosted Customer Data only where necessary to provide, maintain, troubleshoot, secure, back up or restore the service, when the Customer instructs us to, or when required by law. Access is role-based, individually authenticated, logged, and limited to what is required for the task.

Backups and recovery. Backups are kept in accordance with the Customer's services agreement and Section 11, and are protected with the same safeguards as live data.

End of service. When a hosting service ends, we return or securely delete the Customer's hosted data in accordance with the services agreement.

8. Business Intelligence and Data Warehouse Platform

Where processing happens. The BI Platform, including any AI models used for AI-assisted queries, runs on infrastructure operated by Logical Solutions in New Zealand data centres. Queries, retrieved Customer records and generated responses are processed on that infrastructure. [If any third-party or hosted model is used for any function, name the provider, the function, and the data sent to it here — otherwise delete this sentence.]

No training on your data. We do not use Customer Data, queries or AI outputs to train, fine-tune, develop, improve, evaluate or benchmark any artificial intelligence or machine-learning model, whether our own or a third party's. Data is used only to answer the query in front of it and is not incorporated into model weights.

Separation between Customers. Each Customer's application instance and data stores are logically separated and run on dedicated virtual machines. Underlying compute resources may be shared across instances; that sharing is at the compute layer only and does not give one Customer's instance access to another Customer's data.

Human access. Our engineers may access Customer Data, queries and logs where necessary to configure, troubleshoot, secure or support the service. Access is role-based, individually authenticated, logged, and limited to what is required for the task.

Accuracy and human oversight. Reports and AI-generated output can be incomplete or incorrect. Output is presented to authorised users as decision support, not as a decision. We do not use the BI Platform to make automated decisions that produce legal effects for an individual or otherwise significantly affect an individual, and we do not permit Customers to configure it to do so.

Restricted purposes. We do not use the BI Platform, and we do not permit it to be used, to make or inform eligibility decisions about individuals — including decisions about credit, insurance, employment, housing, tenancy, education, immigration status or government benefits — or for surveillance, profiling of individuals for advertising purposes, or facial recognition.

9. Disclosure and third-party service providers

We disclose personal information only:

- to the Customer whose data it is;
- to trusted third-party service providers who help us run our business and deliver our services — for example data centre facility operators, backup and security providers, software vendors, email and communications providers, and our accounting and practice-management systems. Each is engaged under terms that limit them to processing on our behalf, prohibit use for their own purposes, and require appropriate security and confidentiality;
- to our professional advisers, such as lawyers, accountants and auditors, under a duty of confidentiality;
- where required or authorised by law, or in response to valid legal process; and
- to a purchaser in connection with a sale of our business, subject to the purchaser agreeing to comparable privacy obligations.

A list of the main third-party providers that process Customer Data is available to Customers on request.

10. Where information is stored, and overseas disclosure

Customer Data in our data centre and hosting services and in the BI Platform is hosted in New Zealand. Some of the third-party providers described in Section 9, such as software-as-a-service tools we use to run our business, may store information outside New Zealand.

Before disclosing personal information outside New Zealand we take the steps required by information privacy principle 12 of the Privacy Act 2020 — that is, we satisfy ourselves that the recipient is subject to comparable privacy safeguards, or we bind the recipient by contract to comparable safeguards. Where the GDPR applies, transfers out of the EEA or UK rely on the European Commission's adequacy decision in respect of New Zealand, or on standard contractual clauses.

11. Retention

We keep personal information only for as long as we need it, and then delete or de-identify it.

Data	Retention
Website enquiries and sales contacts	[24] months from last contact, unless a contract results
Customer contract, billing and tax records	7 years, as required by NZ tax law
Support tickets and service records	Term of the agreement plus [12] months
Hosted Customer Data	As specified in the Customer's services agreement; returned or deleted within [30] days of termination
Customer Data in the BI Platform	As specified in the Customer's services agreement; returned or deleted within [30] days of termination
BI Platform queries, AI outputs and audit logs	[12] months, then deleted or de-identified

Data	Retention
Security, access and system logs	[90] days, or longer where required for an active investigation
Backups	As specified in the Customer's services agreement; for our own systems, [35] days, after which deleted data is purged from backup media

Where we are required by law to retain information we would otherwise delete, we isolate it, stop actively processing it, and delete it once the obligation ends.

12. Security

We maintain administrative, physical and technical safeguards designed to meet or exceed industry standards for the sensitivity of the information we hold, to comply with applicable privacy and data security law, and to prevent unauthorised access, alteration, disclosure, loss or destruction. These include:

- encryption of data in transit (TLS 1.2 or higher) and at rest;
- role-based access control, unique named accounts and mandatory multi-factor authentication for all administrative access;
- physical access controls at our data centre facilities;
- logical separation of Customer environments, with per-Customer virtual machines and data stores;
- centralised logging, alerting and retention of audit trails;
- patch and vulnerability management, with periodic vulnerability assessment;
- documented change control, backup and disaster recovery procedures;
- background-checked personnel bound by confidentiality obligations, with privacy and security training; and
- an incident response plan that is tested periodically.

Breach notification. If a privacy breach occurs that is likely to cause serious harm, we will notify the Office of the Privacy Commissioner and affected individuals as required by the Privacy Act 2020. Where the breach affects Customer Data, we will notify the affected Customer without undue delay.

13. Your rights

Under the Privacy Act 2020 you may ask us to confirm whether we hold personal information about you, to give you access to it, and to correct it if it is wrong. Where the GDPR applies to our processing, you may also have rights to deletion, portability, restriction, objection, and to withdraw consent.

To make a request, contact our Privacy Officer using the details in Section 17. We will:

- acknowledge your request promptly and respond within 20 working days (Privacy Act) or one month (GDPR), and tell you if we need longer;
- verify your identity before acting, using the minimum information necessary; and
- tell you the reason if we decline any part of a request, and explain how to complain.

If your information is held by us on behalf of a Customer, we will tell you who that Customer is (where we are permitted to) and refer your request to them, or act on their instructions.

Making a request costs nothing in ordinary cases.

14. Cookies and website analytics

Our website uses cookies that are strictly necessary for it to function, and [analytics cookies / no analytics cookies]. [If analytics are used, name the tool here, for example Google Analytics.] Where consent is required in your jurisdiction, we ask for it before setting non-essential cookies, and non-essential cookies are off by default. You can control cookies through your browser settings.

15. Children

Our services are provided to businesses and are not directed to children. We do not knowingly collect personal information from anyone under 16 for our own purposes. If we learn we have collected such information, we will delete it.

16. Changes to this policy

We will update this policy when our practices change. The version number and last-updated date at the top will change, and we will keep prior versions available on request. Where a change materially affects how we handle personal information, we will notify affected Customers in advance.

17. Contact us

If you have any questions about this policy or how we handle personal information, please contact our Privacy Officer:

Privacy Officer, Logical Solutions 2020 Limited
Email: [privacy@logicalsolutions.co.nz]
Phone: [07 XXX XXXX]
Post: [Street address], Hamilton, New Zealand

18. Complaints

If you are not satisfied with our response, you may complain to:

Office of the Privacy Commissioner (New Zealand)
Freephone 0800 803 909 — enquiries@privacy.org.nz — www.privacy.org.nz

If the GDPR applies to you, you may also complain to your local supervisory authority.