



MCS COMMUNICATIONS PTY LTD

PRIVACY POLICY

Effective Date: 1 July 2026

Entity: MCS Communications Pty Ltd

ACN: 616 885 995

1. About this Privacy Policy

MCS Communications Pty Ltd ("MCS Communications", "MCS", "we", "us" or "our") is committed to protecting the privacy and security of personal information that we collect, use, hold and disclose in connection with our business.

MCS provides telecommunications, communications and technology services, including business voice and cloud communications, hosted and cloud PBX services, data and internet services, mobile services, managed technology services, communications analytics, call recording, artificial intelligence ("AI") and related technology solutions.

This Privacy Policy explains how we handle personal information and how we seek to comply with applicable Australian privacy laws, including the **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles ("APPs")**, where applicable.

This Privacy Policy should be read together with our Customer Terms, service agreements, proposals and other contractual documents.

Our Customer Terms contain additional provisions relating to information sharing, credit information, telecommunications services and our relationships with wholesale suppliers and service providers.

2. What is personal information?

"Personal information" generally means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is recorded in material form or not.

Depending on the services we provide, personal information may include:

- name;
- business contact details;
- residential or business address;
- telephone numbers;
- email addresses;
- usernames and account information;
- billing and payment information;
- identification information;
- account and service history;
- information relating to telecommunications services;
- information contained in communications with us;
- call records and call metadata;
- recordings of telephone calls;
- voicemail messages;

- meeting recordings;
- call transcripts;
- AI-generated summaries;
- communications analytics;
- information generated through use of our cloud communications systems;
- IP addresses and device information;
- information relating to service usage;
- information provided through our website, forms or customer portals;
- information contained in support requests;
- information relating to employees or authorised users of our customers; and
- other information that may reasonably identify an individual.

Where appropriate, we may also handle information that is not personal information because it relates solely to a business entity rather than an identifiable individual.

3. How we collect personal information

We may collect personal information directly from you or from other sources.

We may collect information when you:

- contact us by telephone, email or other communication method;
- request a quotation or proposal;
- become an MCS customer;
- purchase or use our services;
- communicate with our support or service teams;
- submit information through our website;
- complete a form or application;
- interact with our online systems or customer portals;
- participate in meetings, demonstrations or consultations;
- provide information relating to authorised users;
- make payments or provide billing information;
- provide information in connection with a service fault or support request; or
- otherwise interact with MCS.

We may also collect information from:

- your employer or organisation;
- authorised representatives;
- telecommunications carriers and wholesale providers;
- technology and software providers;
- cloud communications platforms;
- payment providers;
- credit providers or credit reporting bodies where permitted;
- publicly available sources;
- service partners and suppliers; and
- other third parties where lawful and appropriate.

Where MCS collects personal information through telephone or other communications, we may provide privacy information at or before collection where reasonably practicable. The OAIC specifically recognises that APP 5 notification may be provided through telephone scripts or subsequent communications where appropriate.

4. Information collected through telecommunications and communications services

Because MCS provides telecommunications and cloud communications services, we may handle information generated through the use of those services.

Depending on the service, this may include:

- telephone numbers;
- caller and recipient numbers;
- call date and time;
- call duration;
- call routing information;
- call queues;
- extension information;
- voicemail information;
- call disposition information;
- service usage information;
- call recordings;
- transcripts;
- communications analytics;
- system and device information;
- IP addresses;
- network information; and
- information relating to users of a customer's communications system.

This information may be collected and processed as necessary to provide, operate, maintain, troubleshoot, secure and improve the relevant service.

Where MCS is providing services to a business customer, the business customer may also determine how certain information concerning its employees, customers or other users is collected and used within its communications system.

5. Call recording

Some MCS services may allow or provide call recording functionality.

Where call recording is enabled, telephone conversations may be recorded for purposes including:

- providing the communications service;
- quality assurance;
- training;
- customer service;
- dispute resolution;
- compliance;
- security;
- record keeping;
- business continuity;
- analysis and reporting; and
- other purposes authorised by the relevant customer or permitted by law.

Customers are responsible for ensuring that their use of call recording functionality complies with applicable laws and that appropriate notices or consents are provided to callers where required.

MCS may provide functionality that allows customers to configure call recording, notifications, retention or access settings.

6. Artificial Intelligence and automated technologies

6.1 Our use of AI

MCS may use artificial intelligence, machine learning, automated processing and related technologies as part of our services.

Examples may include:

- AI receptionists and virtual agents;
- automated call answering;
- conversational AI;
- speech recognition;
- speech-to-text transcription;
- call summarisation;
- sentiment or interaction analysis;
- call categorisation;

- automated call disposition;
- communications analytics;
- automated quality assurance;
- AI-assisted customer service;
- AI-assisted reporting;
- fraud, security and anomaly detection;
- automated workflow tools;
- document and information processing; and
- AI features provided by third-party cloud communications platforms.

AI technologies may process information contained in telephone calls, meetings, messages, voicemails, transcripts, customer interactions and other communications.

6.2 AI-generated transcripts and summaries

Where an AI-enabled service is used, communications may be converted into text or analysed to produce:

- transcripts;
- summaries;
- action items;
- call notes;
- classifications;
- keywords;
- sentiment or interaction indicators;
- quality scores;
- analytics;
- reports; or
- other AI-generated information.

AI-generated information may contain personal information where the underlying communication identifies or relates to an individual.

MCS treats such information as personal information where applicable and seeks to handle it in accordance with applicable privacy obligations.

6.3 AI service providers

MCS may use third-party technology providers to deliver AI-enabled services.

These providers may include:

- cloud communications platforms;
- telecommunications providers;
- speech recognition providers;
- AI model providers;
- cloud hosting providers;
- analytics providers;
- CRM platforms;
- customer service platforms; and
- other technology suppliers.

Depending on the service, information may be processed by these providers on MCS's behalf or on behalf of the MCS customer.

The specific third-party provider may vary depending on the technology solution selected by the customer.

6.4 AI training

Unless expressly agreed otherwise, MCS does not intend to use customer communications or personal information for the purpose of training a general-purpose AI model unrelated to the provision of the relevant service.

Where an underlying third-party platform has its own AI processing or model-training arrangements, the applicable service provider's terms and privacy documentation may also apply.

MCS will seek to use contractual and technical controls appropriate to the services we provide to manage how customer information is processed by third-party providers.

6.5 AI decision-making

MCS may use automated systems to assist with communications processing, routing, classification, analytics, security and customer service.

Where practical and appropriate, automated systems are intended to assist rather than replace human decision-making.

MCS does not generally intend to make significant decisions about individuals solely through automated processing.

Where automated processing could have a significant effect on an individual, MCS will consider the applicable legal requirements and the circumstances of the processing.

6.6 Accuracy of AI-generated information

AI-generated transcripts, summaries, classifications and analytics may contain errors.

AI-generated information should therefore not automatically be treated as a definitive record of what an individual said or intended.

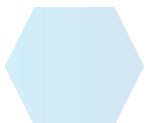
Customers should consider appropriate human review where AI-generated information is used for important business, employment, legal, financial, compliance or customer-service decisions.

7. How we use personal information

We may collect, hold, use and disclose personal information for purposes including:

- providing telecommunications services;
- providing cloud communications services;
- provisioning and managing telephone numbers;
- providing internet and data services;
- providing mobile services;
- providing hosted PBX and cloud PBX services;
- managing customer accounts;
- processing orders;
- providing technical support;
- monitoring and maintaining services;
- diagnosing faults;
- managing network performance;
- managing service security;
- processing payments and billing;
- managing credit;
- preventing fraud or misuse;
- maintaining business records;
- responding to enquiries;
- managing complaints;
- providing customer service;
- recording and analysing communications where enabled;
- providing AI and analytics functionality;
- improving our services;
- managing suppliers and technology partners;
- meeting legal and regulatory obligations;
- enforcing contractual rights;
- protecting our business, systems and customers; and
- communicating with customers about relevant products and services.

We may also use de-identified, aggregated or statistical information for business analysis, reporting and service improvement where reasonably appropriate.



8. Disclosure of personal information

We may disclose personal information where reasonably necessary to provide our services or operate our business.

Recipients may include:

Telecommunications providers

We may disclose relevant information to carriers, wholesale telecommunications providers and network operators for purposes including provisioning, maintaining, supporting and managing telecommunications services.

Our existing Customer Terms contemplate the disclosure of customer details and service information to wholesale suppliers where required to facilitate carriage services.

Technology providers

We may disclose information to providers of:

- cloud communications platforms;
- PBX platforms;
- AI services;
- call recording platforms;
- transcription services;
- analytics platforms;
- CRM systems;
- IT management systems;
- cybersecurity services;
- cloud hosting services;
- backup services; and
- other software or technology services.

Professional advisers

Information may be disclosed to:

- accountants;
- lawyers;
- auditors;
- insurers;
- financial institutions;
- consultants; and
- other professional advisers.

Government and regulatory bodies

We may disclose information where required or authorised by law, regulation, court order or other lawful authority.

Business transfers

If MCS is involved in a merger, acquisition, restructuring, sale of assets or similar transaction, personal information may be transferred as part of that transaction where permitted by law.

9. Overseas disclosure and cloud services

MCS may use service providers that store or process information outside Australia.

This may occur where our telecommunications, cloud, AI, software, hosting, analytics, cybersecurity or other technology providers operate international infrastructure.

Depending on the services used, personal information may be processed in countries including Australia, the United States, New Zealand, Singapore, the United Kingdom or other jurisdictions in which our technology providers operate.

The specific location of processing may change as providers modify or expand their infrastructure.

Where applicable, MCS will take reasonable steps required under the Privacy Act and APP 8 in relation to overseas disclosures.

Our privacy collection notices may provide more specific information where the particular service involves overseas processing.

10. Direct marketing

MCS may use personal information to communicate with customers and prospective customers about products, services, upgrades, offers, service changes and other information relevant to their relationship with MCS.

We will comply with applicable privacy and direct-marketing requirements.

Where required, individuals will be provided with an opportunity to opt out of receiving direct marketing communications.

An individual may request that MCS stop using their personal information for direct marketing by contacting us using the details set out in this Policy.

11. Cookies, websites and online services

When you visit our website or use our online services, we may collect information such as:

- IP address;
- browser type;
- device information;
- operating system;
- pages viewed;
- date and time of access;
- referring website;
- approximate location information;
- website interaction information; and
- other technical information.

We may use cookies, analytics technologies and similar tools to operate, secure and improve our website and services. Third-party services used on our website may also collect information in accordance with their own privacy policies.

12. Security of personal information

MCS takes reasonable steps to protect personal information against:

- misuse;
- interference;
- loss;
- unauthorised access;
- unauthorised modification; and
- unauthorised disclosure.

Depending on the nature of the information and services involved, security measures may include:

- access controls;
- authentication;
- user permissions;
- encryption;
- secure cloud platforms;
- network security;
- endpoint security;
- monitoring;
- logging;
- backups;
- physical security;
- staff and contractor controls;
- supplier security requirements; and
- incident response procedures.

No electronic system can be guaranteed to be completely secure.

13. Data retention

MCS retains personal information only for as long as reasonably necessary for the purposes for which it was collected, to provide services, comply with legal or contractual obligations, resolve disputes, maintain business records, protect our legitimate interests or otherwise as permitted by law.

Retention periods may differ depending on the type of information.

For example, telecommunications records, billing information, service records, support records, call recordings, transcripts and AI-generated information may each have different retention requirements.

Where personal information is no longer required and there is no legal or business requirement to retain it, MCS may securely delete or de-identify it.

Customers using MCS services may also have configuration options relating to the retention of call recordings, transcripts and other communications data.

14. Access to personal information

Individuals may request access to personal information that MCS holds about them.

Requests should be made using the contact details in this Privacy Policy.

We may need to verify the identity of the person making an access request before providing information.

In some circumstances, we may refuse access where permitted or required by law.

Where access is refused, we will generally provide an explanation where legally permitted.

15. Correction of personal information

MCS takes reasonable steps to ensure personal information is accurate, complete and up to date.

If you believe information we hold about you is inaccurate, incomplete or out of date, you may request that we correct it.

We may ask for reasonable information to verify the requested correction.

16. Privacy complaints

If you believe MCS has mishandled your personal information or breached applicable privacy requirements, you may make a privacy complaint.

Complaints should include:

- your name;
- contact details;
- a description of the issue;
- relevant dates;
- relevant documents or information; and
- the outcome you are seeking.

MCS will investigate privacy complaints and seek to respond within a reasonable period.

We will endeavour to resolve privacy complaints directly with the individual.

If you are not satisfied with our response, you may have the right to contact the **Office of the Australian Information Commissioner (OAIC)**.

17. Data breaches and security incidents

MCS maintains procedures for identifying, assessing and responding to suspected data breaches and security incidents.

A data breach may involve:

- unauthorised access;
- unauthorised disclosure;
- loss of personal information;
- compromised credentials;
- cyberattack;
- ransomware;
- accidental disclosure; or
- another event affecting personal information.

Where the **Notifiable Data Breaches Scheme** applies and an eligible data breach is identified, MCS will comply with applicable notification requirements.

The NDB scheme requires covered entities to notify affected individuals and the OAIC where a breach is likely to result in serious harm.

18. Telecommunications and regulatory requirements

As a telecommunications and communications technology provider, MCS may be required to collect, use, retain or disclose information to comply with applicable telecommunications legislation, regulatory requirements, lawful requests, court orders or other legal obligations.

These obligations may apply independently of this Privacy Policy.

Our Customer Terms contain additional provisions concerning telecommunications services, wholesale suppliers, credit information and regulatory requirements.

19. Credit information

Where MCS provides credit or payment terms, we may collect, use and disclose information relevant to credit management where permitted by applicable law.

This may include:

- information required to assess creditworthiness;
- payment history;
- account information;
- information obtained from credit reporting bodies; and
- information obtained from other credit providers.

Our Customer Terms contain additional provisions concerning credit information and credit reporting.

20. Business customers and authorised users

Many MCS services are supplied to businesses rather than directly to individual consumers.

Where a business customer provides MCS with personal information relating to its employees, contractors, customers or other authorised users, the business customer is responsible for ensuring that it has the appropriate authority to provide that information to MCS.

This may include ensuring that individuals have been appropriately informed about:

- call recording;
- communications monitoring;
- AI processing;
- transcription;
- analytics;
- CRM integrations;
- service monitoring; and
- other relevant processing.

MCS will handle information received from business customers in accordance with applicable contractual and privacy obligations.

21. Third-party platforms and integrations

MCS may integrate telecommunications and communications services with third-party systems selected by customers.

Examples may include:

- CRM platforms;
- Microsoft 365;
- Google Workspace;
- Salesforce;
- service management systems;
- accounting platforms;
- customer databases;
- AI platforms;
- analytics platforms; and
- other business applications.

When a customer requests an integration, information may be transferred between MCS services and the third-party platform.

Customers should review the privacy practices and terms of the relevant third-party provider.

22. Sensitive information

Sensitive information receives additional protection under Australian privacy law.

MCS does not generally seek to collect sensitive information unless it is reasonably necessary for our functions or services and collection is permitted by law.

Because communications services may involve conversations between individuals, it is possible that sensitive information may be incidentally contained within a telephone call, recording, transcript, voicemail or other communication.

Where MCS handles such information, we will seek to manage it in accordance with applicable privacy obligations.

23. Children's privacy

MCS's services are primarily business and commercial services.

We do not generally intentionally collect personal information from children as a target audience.

If we become aware that personal information relating to a child has been collected in circumstances where it should not have been, we may take appropriate steps to delete or otherwise manage the information.

24. De-identified and aggregated information

MCS may use information that has been aggregated or de-identified for purposes such as:

- service performance analysis;
- telecommunications reporting;
- system improvement;
- operational analysis;
- business planning;
- statistical reporting; and
- security analysis.

Where information has been properly de-identified so that individuals are no longer reasonably identifiable, it may no longer constitute personal information for the purposes of the Privacy Act.

25. Changes to this Privacy Policy

MCS may update this Privacy Policy from time to time.

Updates may be made to reflect:

- changes to our services;
- new technology;
- AI functionality;
- changes to our suppliers;
- changes to applicable law;
- regulatory guidance;
- changes to our business practices; or
- improvements to our privacy practices.

The latest version will be made available through our website or otherwise provided to customers where appropriate.

26. Contacting MCS about privacy

If you have a question, access request, correction request or privacy complaint, please contact MCS Communications using our current published business contact details.

MCS Communications Pty Ltd

ACN: 616 885 995

Privacy Contact: [INSERT PRIVACY EMAIL ADDRESS]

Telephone: [INSERT PHONE NUMBER]

Website: [INSERT WEBSITE]

Postal Address: [INSERT BUSINESS ADDRESS]

Please include "Privacy" in the subject line of written correspondence where possible.

27. External privacy regulator

If you are not satisfied with our response to a privacy complaint, you may contact the:

Office of the Australian Information Commissioner (OAIC)

Website: www.oaic.gov.au

Telephone: 1300 363 992

The OAIC administers Australia's federal privacy framework and the Australian Privacy Principles.

28. Relationship with other MCS documents

This Privacy Policy forms part of MCS's broader privacy, security and information-management framework.

It should be read together with, where applicable:

- MCS Customer Terms;
- MCS service agreements;
- MCS proposals and statements of work;
- MCS acceptable use requirements;
- applicable telecommunications provider terms;
- third-party platform terms;
- third-party privacy policies; and
- customer-specific service documentation.

Where there is a conflict between this Privacy Policy and a specific contractual agreement, the contractual agreement will apply to the extent permitted by law.

Version Control

Document: MCS Communications Privacy Policy

Effective Date: 7 September 2026

Review Date: September 2027

Owner: MCS Communications Pty Ltd

ACN: 616 885 995