Yomojo®

Privacy Policy

Last updated: 19 October 2026

	IN SHORT	1
1	ABOUT THIS POLICY	1
2	WHAT INFORMATION DO WE COLLECT?	1
3	HOW DO WE COLLECT IT?	1
4	HOW DO WE USE IT?	2
5	HOW DO WE CHECK YOUR IDENTITY?	2
6	CREDIT CHECKS AND CREDIT REPORTING	2
7	DECISIONS MADE BY COMPUTER PROGRAMS	2
8	WHO DO WE SHARE IT WITH?	3
9	WHERE IS YOUR INFORMATION HELD, AND WHO CAN SEE IT FROM OVERSEAS?	3
10	HOW DO WE PROTECT YOUR INFORMATION, AND HOW LONG DO WE KEEP IT?	3
11	CHILDREN AND YOUNG PEOPLE	4
12	HOW CAN YOU SEE OR CORRECT YOUR INFORMATION?	4
13	HOW DO YOU MAKE A PRIVACY COMPLAINT?	4
14	CHANGES TO THIS POLICY, AND HOW TO CONTACT US	4

IN SHORT

This is a summary. The full policy follows, and it is the full policy that applies.

- We collect the information we need to set up, supply and bill your services, and the information the law requires a telecommunications provider to collect.
- We check your identity when the law requires or allows it. We ask for your consent before we check an identity document electronically.
- If you apply for a service that you use before you pay for it, such as a postpaid service, we may run a credit check, and we will tell you first.
- A computer program may make some decisions, such as whether to accept an application for a postpaid service. You can ask for a person to review a decision.
- Our core customer systems are in Australia. Teams in the Philippines and Sri Lanka work for us and can see your information.
- You can opt out of marketing at any time.
- You can ask to see or correct your information. If you are unhappy with how we have handled it, you can complain to us, and then to the Telecommunications Industry Ombudsman or the Office of the Australian Information Commissioner.

1 ABOUT THIS POLICY

This Privacy Policy ("Policy") explains how Yomojo Pty Ltd (ACN 609 279 245) ("Yomojo", "we", "us") collects, holds, uses and shares personal information when you use our website, our mobile applications, and our products and services (together, the "Services").

It applies to our customers, to people who apply for our Services, to the people who use Services on a customer's account ("End-users"), to authorised representatives, and to visitors to our website and apps.

We are bound by the Privacy Act 1988 (Cth) and the Australian Privacy Principles. As a supplier of telecommunications services we also have obligations under other laws, regulations and industry codes, including the Telecommunications Act 1997 (Cth). Where we supply a service on credit, we are also a credit provider under Part IIIA of the Privacy Act. Our Credit Reporting Policy, available at https://www.yomojo.com.au/terms, explains how we handle credit information and forms part of this Policy.

2 WHAT INFORMATION DO WE COLLECT?

We collect the information we need to supply our Services to you, and the information the law requires us to collect.

Account details: your name, contact number, email address, password and date of birth, your home address, and a delivery address if it is different.

Identity information: details from identity documents, where the law requires or allows us to check your identity. See section 5.

Biometric information: if you choose to verify your identity with a face check, a photo of your identity document and a photo or short video of your face. Biometric information is sensitive information, and we only collect it with your express consent. See section 5.

Service and usage information: details of how you use our Services, including the numbers you call or message, the time and length of your calls, the location they are made from, and the amount of data you use. If you bring a mobile number to us from another provider, we collect the number, the name of that provider and the details that identify your account with it. The law requires us to keep some of this information.

Payment information: your payment method details, and your billing and payment history with us. We do not store your payment method details ourselves. We give them to payment gateways that comply with the Payment Card Industry standard, which store and process them.

Credit information: if you apply for or use a service that we supply on credit, information about your credit history, including a credit report. See section 6.

Support records: what you tell us by email, by phone or in online chat, including recordings of your calls with us. We keep this as a record of what you asked us and what we did, for quality and service assurance.

End-user details: the name and date of birth of each person you add to your account.

Authorised representative details: the full name and email address of anyone you authorise to manage your account. Please let them know that you have given us their details.

Website and app information: information such as your IP address, internet service provider, browser type, operating system and language, the pages you visit, the links you click, your search terms, how you scroll and click through a page, and the date and time of your visit. We collect this automatically, using cookies and similar technologies, through tools such as Google Analytics, Google Ads and Microsoft Clarity. Some of these tools record a replay of how you used a page, with the details you type hidden. It is pseudonymised or aggregated where practicable. You can manage cookies through your browser settings, although turning some cookies off may affect how our website works.

Sign-in information: if we offer sign-in through Facebook or Google and you choose to use it, we exchange authentication information with that service, such as your email address.

App fingerprint and face sign in: if you turn on fingerprint or face sign in to the Yomojo app, your phone checks your fingerprint or face. We do not receive or keep it. Your phone only tells the app whether the check succeeded.

Surveys, competitions and feedback: the information you give us when you take part.

Apart from biometric information for an optional face check, we do not generally need sensitive information, such as information about your health, to supply our Services. If we need to collect it, we will ask for your consent separately, unless the law requires or allows us to collect it without consent, and you can withdraw your consent at any time. We do not use sensitive information for direct marketing.

3 HOW DO WE COLLECT IT?

We collect most information directly from you, when you:

- register as a customer or apply for a Service;
- use our Services;
- contact us with a question or comment;
- pay a bill;

- enter a competition or promotion, or take part in market research; or
- cancel a Service.

We also collect information from:

- the account holder, if you are an End-user or an authorised representative;
- a credit reporting body or a business that provides information about commercial credit worthiness, where you apply for or use a service that we supply on credit;
- identity verification and Digital ID providers, fraud prevention providers, and document issuers or official record holders;
- business directories and other public sources; and
- other authorised third parties, where the law allows it.

When we collect your information, or as soon as practicable afterwards, we will take reasonable steps to tell you why we are collecting it and whether the law requires it. We will also tell you how it may be used or disclosed, and how you can access it, correct it or complain about how it is handled.

If you do not give us the information we ask for, we may not be able to supply a Service to you.

4 HOW DO WE USE IT?

We use your information to:

- supply, manage and bill your Services, and send you information about them;
- confirm your identity and keep your account secure;
- decide whether to accept an application or order, including by checking our records of any previous account you have had with us, for example whether an amount was left unpaid or there was fraud or misuse;
- assess whether to supply you with a service on credit, and recover amounts owed to us;
- answer your questions and investigate complaints;
- prevent, detect and investigate crime, fraud and money laundering;
- meet our legal obligations, including under industry codes and standards, and requests from law enforcement agencies;
- plan and improve our business, products and services, including by analysing the market, producing reports and asking for your opinions;
- advertise our products and services to you online, and measure how well that advertising works;
- get legal or financial advice; and
- tell you about our products, offers and promotions.

If you are our customer, we may send you marketing messages about our products and services. You can opt out at any time, using the unsubscribe option in the message, the settings in your dashboard, or by contacting us. We will still send you the messages we need to send about your account, billing, security or Services.

5 HOW DO WE CHECK YOUR IDENTITY?

To provide or protect a telecommunications service, we may be required or permitted by law to collect identity information. This may include your full legal name, date of birth, residential address, and details from government-issued identity documents such as a driver licence, passport or Medicare card.

We may ask for this information when you apply for or activate a Service, port a mobile number, ask for access to account information, replace a SIM, change account ownership, update sensitive account details or carry out another high-risk transaction. If we cannot establish your identity, we will not be able to supply the Service.

Before we check identity document information electronically with the relevant document issuer or official record holder through third party systems, we will ask for your express consent. We will give you information about the check before we ask. Our Identity Verification Requirements are published on our website.

For some checks, where we offer it, you can choose to verify your identity with a face check. You take a photo of your identity document and then a photo or short video of your face with your phone. Our identity verification provider compares your face with the photo on the document, checks that a real person is present, and tells us the result. We will ask for your express consent first, and tell you before the check who runs it, where the images are processed and how long they are kept. We use this information only to verify your identity and prevent fraud. If you do not want a face check, we will offer another way to verify your identity where one is available.

Personal information collected specifically for an electronic identity verification check will be used or disclosed only for identity verification, fraud prevention, account security, legal or regulatory compliance, audit, complaint handling and dispute resolution. It will not be used for customer profiling, tracking for unrelated purposes, direct marketing, advertising, promotion, offering additional goods or services, or market research.

We may keep a record of your consent, the verification method used, the date and time of the check, the outcome, a transaction or audit reference, and limited supporting information needed to resolve an unsuccessful or disputed check.

Where identity information is collected solely to complete an identity check for activation of a prepaid mobile service, we do not make or keep a copy of the identity document. We also do not keep its government document number after verification. The only exception is where the law requires or authorises us to keep them.

6 CREDIT CHECKS AND CREDIT REPORTING

Some of our services are supplied on credit, which means you use the service before you pay for it. Before we supply one, we may run a credit check, and we will tell you first. We may get a credit report about you from a credit reporting body. We may also give it information about you, including if you do not pay an amount you owe us or you commit a serious credit infringement.

The credit reporting body we deal with is Experian Data Registries Pty Ltd (Experian). Experian can be contacted on 1300 783 684 or at www.experian.com.au.

Our Credit Reporting Policy explains what credit information we hold, how we use it, who we share it with, your rights and how to complain. It is available at https://www.yomojo.com.au/terms.

7 DECISIONS MADE BY COMPUTER PROGRAMS

We use computer programs to make, or to help make, some decisions that could significantly affect you.

The following decisions may be made by a computer program on its own, with no person involved:

- whether to accept your application for a service that we supply on credit;
- whether to decline an application or stop an order because of a previous account with us, for example where an amount was left unpaid or there was fraud or misuse;
- whether to hold an order for further checks, for example where it does not pass a fraud or compliance check;
- whether to stop a transfer of a mobile number to us that cannot be verified;
- whether to restrict or suspend a Service because an amount is unpaid;
- whether to block further chargeable use of a Service that has reached its credit limit;
- whether to restrict calls on a Service because of unusual usage that may be fraudulent;
- whether to renew your Plan when the payment for it fails; and
- whether to cancel a Service that has had no Plan, usage, top up or payment for 90 days.

For a credit application, the program applies criteria that we set to the credit report we receive about you, such as a minimum credit score, how long your credit file has existed and whether it shows any defaults.

For an application or order, the program also checks our records of any previous account you have had with us. A senior staff member can review and override a decision to decline it.

A decision to cancel a Service because of an unpaid debt is made by a person.

Computer programs also help our staff to make other decisions, including decisions about credit applications that a person assesses, identity verification, whether a Service is available at your address, and the prevention of fraud and financial crime. Some identity verification and fraud decisions may also be made with no person involved.

These programs use your account, identity, payment and usage information, our records of any previous account you have had with us and, for a credit application, the credit reporting information we receive about you.

If you have a question or concern about one of these decisions, you can contact us and ask for it to be reviewed by a person.

8 WHO DO WE SHARE IT WITH?

We only give your information to others as described in this Policy, where you have agreed, or where the law requires or allows it. The people and organisations we may give it to include:

- our related companies, and the companies that run our customer service, credit and accounts operations for us;
- our technology, delivery and other service providers;
- our wholesale network and service suppliers, and the technicians we engage to make sure your Service is working;
- other telecommunications providers, when you move a service to or from us;
- payment gateways and banks;
- identity verification and Digital ID providers, document issuers and official record holders that assist us to verify identity;
- fraud prevention and authorised security agencies;
- credit reporting bodies;
- debt collectors that recover amounts owed to us on our behalf;
- our professional advisers, such as our auditors, accountants and lawyers;
- market research and customer review organisations;
- our website analytics and digital advertising providers;
- your authorised representative, and anyone else who has legal authority to act for you, such as a guardian, attorney or executor;
- the account holder, if you are an End-user;
- emergency services, and the operator of the Integrated Public Number Database (IPND); and
- the Telecommunications Industry Ombudsman, regulators, government agencies and law enforcement agencies.

If you sign in using Facebook or Google, or post in a forum or on a social media page that we use, that service's own privacy policy applies to the information you give it.

9 WHERE IS YOUR INFORMATION HELD, AND WHO CAN SEE IT FROM OVERSEAS?

Our core customer systems are hosted in Australia.

Our customer service, credit and accounts teams are located in the Philippines, where they are engaged for us through an outsourcing company. We also have a small number of sales and technical staff in Sri Lanka. People in those countries may access your personal information in order to provide the Services to you. Outside Australia, only authorised staff in the Philippines and Sri Lanka can access credit reports and credit scores.

Some of our technology service providers may also process information outside Australia. Our website analytics and digital advertising providers (such as Google and Microsoft) may process limited web and app usage information on servers located overseas, including in the United States. Where another overseas location is relevant to a particular identity verification or Digital ID service, we will identify that country in the applicable collection notice or this Policy, where practicable, before the check occurs.

We take reasonable steps to make sure overseas staff and service providers handle your information in line with the Australian Privacy Principles.

10 HOW DO WE PROTECT YOUR INFORMATION, AND HOW LONG DO WE KEEP IT?

We use technical and organisational measures to protect personal information from misuse, interference, loss and unauthorised access, modification or disclosure. These measures include:

- identity checks and, for high-risk telecommunications transactions, multi-factor authentication;
- controlled logins and authorisation levels, so that staff can only access the information their job requires;

- logging access and changes to customer records under the staff member who made them, and auditing that activity from time to time;
- restrictions on copying, printing, recording and transferring information; and
- regular privacy training, monitoring and quality assessment of our staff.

No method of sending information over the internet is completely secure. If a data breach is likely to result in serious harm to you, we will notify you and the Office of the Australian Information Commissioner, as the law requires.

We keep your information for as long as we need it to provide the Services, to manage your account and any amounts owing, to resolve complaints, and to meet our legal obligations. Different laws require us to keep different records for different periods. For example, billing records are kept for at least six years, and our network supplier keeps certain telecommunications data for at least two years. If an account was closed with an amount unpaid, or because of fraud or misuse, we keep a record of that for 7 years after the account closed, so that we can assess any new application. When we no longer need information, we securely destroy it or remove the details that identify you.

11 CHILDREN AND YOUNG PEOPLE

You must be 18 or over to hold a Yomojo account. Adults can add their children to their account as End-users. If you add someone who is under 18, you confirm that you are their parent or guardian, or have their parent's or guardian's authority, and that you consent on their behalf to us handling their information as set out in this Policy. For anyone under 15, we rely on the consent of their parent or guardian.

We do not ask anyone under 18 to contact us or to give us personal information. If a child does contact us, we only collect the information included in that communication.

A parent, guardian or account holder can contact privacy@yomojo.com.au to ask about, access or correct personal information about a child. We will check identity and authority first.

12 HOW CAN YOU SEE OR CORRECT YOUR INFORMATION?

You can see some of your information, and update your personal details, by logging in to your dashboard.

You can also ask us for a copy of the personal information we hold about you, or ask us to correct it, by emailing privacy@yomojo.com.au or through our Contact Us page at https://www.yomojo.com.au/contact-us. We will confirm your identity before we act on a request. We aim to acknowledge a request within 7 days, and we will respond within 30 days. We do not charge you for making a request. If we refuse a request, we will tell you why in writing, and how you can complain.

Please let us know if your details change, for example your address, so that we can keep our records up to date.

13 HOW DO YOU MAKE A PRIVACY COMPLAINT?

If you think we have mishandled your personal information, or breached the Privacy Act or the Australian Privacy Principles, please email privacy@yomojo.com.au with the details. You can also call us or write to us using the details in section 14.

We will acknowledge your complaint within 2 working days. We will tell you our proposed resolution within 10 working days, or explain why we need longer and give you a new timeframe. In every case we will give you a written response within 30 days. We do not charge you for making a complaint or for handling it.

If you are not satisfied with our response, you can contact:

- the Telecommunications Industry Ombudsman on 1800 062 058 or at www.tio.com.au; or
- the Office of the Australian Information Commissioner on 1300 363 992 or at www.oaic.gov.au.

Complaints about our Services that are not about privacy can be emailed to complaints@yomojo.com.au. Our Complaints Handling Policy is available at https://www.yomojo.com.au/complaint.

14 CHANGES TO THIS POLICY, AND HOW TO CONTACT US

We may update this Policy from time to time. The current version is always available at https://www.yomojo.com.au/terms. The date at the top of this Policy shows when it was last updated, and we keep a record of each previous version. You can ask us for a copy in another form, such as a printed copy, and we will give it to you free of charge.

Yomojo Pty Ltd (ACN 609 279 245)
Phone: 1300 YOMOJO (1300 966 656)
International: +61 2 8089 1602
Privacy enquiries: privacy@yomojo.com.au
General enquiries: support@yomojo.com.au
Complaints: complaints@yomojo.com.au
Address: Level 5, 121 Walker Street, North Sydney NSW 2060
Website: https://www.yomojo.com.au