

# Privacy Policy

**Last reviewed:** May 2026

This privacy policy (the “Privacy Policy”) applies to Paytime Services Pty Ltd ACN 647 450 137, and its affiliates and related companies (together, “Paytime”, “we”, “us” or “our”). It explains how we collect, hold, use, disclose and protect personal information, including personal information collected through our websites, mobile applications, email, cloud-based services, and any widgets we embed in third-party platforms with a link to this Privacy Policy (“Websites”).

Paytime is bound by the Privacy Act 1988 (Cth) (“Privacy Act”), including the Australian Privacy Principles (“APPs”) in Schedule 1, the Notifiable Data Breaches scheme, and the amendments made by the Privacy and Other Legislation Amendment Act 2024. This policy is published to satisfy our obligations under APP 1.

By “personal information” we mean information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not and whether it is recorded in a material form or not. Personal information does not include information that has been effectively de-identified.

Our third-party suppliers and commercial partners (“our Partners”) are independent of Paytime and have their own privacy practices. We are not responsible for their handling of personal information. Where our Websites contain links to third-party sites, those sites are not under our control and this Privacy Policy does not apply to them.

We may amend this Privacy Policy from time to time. The current version is always available on our Website and the date at the top of this policy will be updated. Where changes are material, we will give you reasonable advance notice by email or in-product notification before they take effect.

## 1. What personal information we collect and why we collect it

The table below sets out the categories of personal information we usually collect, examples of what each category includes, and the purposes for which we collect, hold, use and disclose that information. We will not use your personal information for a purpose other than one of these primary purposes (or a closely related secondary purpose you would reasonably expect) unless you consent, or we are required or authorised by law to do so.

Category of information	Examples	Purpose(s) of collection
Identity & contact	Name, date of birth, residential address, geolocation, phone, email, government identifiers (e.g. driver licence) where required	Establishing and administering your Paytime account; verifying your identity; meeting our obligations under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth); communicating with you about your account; preventing fraud and misuse.
Employment & payroll	Employer name, position, employment status, salary, leave balances, terminations, variations	Calculating your accrued earnings and entitlements made available through Paytime Services; reconciling withdrawals against

Category of information	Examples	Purpose(s) of collection
	to employment, payroll/HRIS records	your pay cycle with your employer; processing transactions on your behalf; responding to your employer in connection with Paytime Services.
Financial	Bank account details, transaction history, fees, repayments	Processing transactions and disbursements you request; collecting fees; producing transaction records and statements; investigating disputes; meeting record-keeping and reporting obligations under financial-services and tax laws.
Device & usage	IP address, device identifiers, operating system, browser type, mobile network information, pages visited, in-app activity, security/fraud signals	Operating, securing and improving the Websites and Paytime Services; diagnosing technical issues; detecting and preventing fraud, misuse and unauthorised access; producing aggregated analytics about usage of our Services.
Marketing preferences	Subscription status, channel preferences, engagement with our communications	Sending you service updates and (where you have not opted out) marketing communications about Paytime products and the products of our Partners; measuring the effectiveness of our communications.
Job applicants & supplier staff	Name, contact details, position, CV/work history, referee information (applicants only)	Assessing your application for employment with Paytime; managing our commercial relationships with suppliers, service providers and Partners.
Support & complaints	Correspondence with our support team, records of phone calls, complaint and dispute records	Responding to your enquiries; handling complaints and disputes; improving our products and the quality of our customer support.

If you do not provide some of the information described above (if needed by us), or we cannot verify it, we may be unable to provide you with Paytime Services, verify your identity, comply with our legal obligations, or otherwise do business with you.

## 2. Sensitive information

Some of the information we collect (for example, government identifiers, biometric information used in an identity check, or health information provided in support of a hardship request) is “sensitive information” under the Privacy Act. We collect sensitive information only where it is reasonably necessary for one of our functions or activities and either you have consented, or the collection is required or authorised by law. We will not use or disclose sensitive information for any purpose other than the purpose for which it was collected, unless you consent or an exception in the Privacy Act applies.

### 3. How we collect personal information

We collect personal information in the following ways:

- Directly from you, when you sign up for Paytime Services, use our Websites or app, contact our customer support team, respond to a survey, enter a competition we run, apply for a job with us, or otherwise communicate with us.
- From your employer or their payroll/HRIS provider, where you have authorised Paytime to receive your employment and payroll information so we can provide Paytime Services.
- From publicly or commercially available sources, where this is necessary to comply with our legal obligations.
- From social media or other third-party accounts you choose to link to your Paytime account. What we receive depends on the privacy settings you have applied with that third party.
- Automatically, when you use our Websites or app, through cookies, pixels, log files and similar technologies (see section 13).

### 4. How we use personal information

We use personal information for the specific purposes set out in section 1. In summary, we use personal information to:

- Provide, administer, secure and improve Paytime Services and the Websites;
- Process the transactions you request and produce records of those transactions;
- Verify your identity, including under anti-money laundering and counter-terrorism financing laws;
- Communicate with you about your account, including service notices and responses to your enquiries;
- Send you marketing where you have not opted out (see section 12);
- Detect, investigate and prevent fraud, misuse and other unlawful activity;
- Conduct analytics to understand how Paytime Services are used and to improve them;
- Consider you for employment with Paytime, if you have applied for a role;
- Comply with our obligations under applicable laws, court orders and regulator requests; and
- Defend or exercise our legal rights.

### 5. Automated decision-making

Paytime uses automated processes (for example, rules-based fraud monitoring and identity verification scoring) to support some decisions about the Paytime Services we provide to you. These automated processes inform human decision-makers; they are not, on their own, used to make decisions that significantly affect your rights or interests.

From 10 December 2026, the Privacy and Other Legislation Amendment Act 2024 will require us to publish additional information about any automated decision-making that does significantly affect individuals' rights or interests (new APP 1.7). Ahead of that commencement, we are reviewing every decision in the

Paytime Services pipeline and will update this section by that date. If we begin using automated decision-making within scope of APP 1.7 before then, we will tell you about it in this policy and in a collection notice.

## 6. How we share personal information with other parties

We may disclose personal information to:

- Our affiliates and related companies, for the purposes described in section 1;
- Our Partners, suppliers and service providers who help us run our business – for example, identity verification, fraud prevention, payment processing, hosting, analytics, communications and customer service providers – who are contractually required to handle your information consistently with this policy;
- Your employer and their payroll/HRIS provider, where this is necessary to deliver Paytime Services or to resolve a complaint;
- Financial institutions we partner with to jointly create or offer a product;
- A purchaser or successor entity, in connection with an actual or proposed merger, acquisition, financing or sale of all or part of our business (in which case the recipient will be required to use your information consistently with this policy);
- Law enforcement, regulators, courts or other government agencies, where the disclosure is required or authorised by law (for example, a subpoena, court order, AUSTRAC reporting obligation, or production notice under the Privacy Act);
- Other third parties where we reasonably believe disclosure is necessary to prevent physical harm or financial loss, to report suspected illegal activity, or to investigate suspected breaches of our terms; and
- Any other third party with your consent or at your direction.

## 7. Disclosure of personal information overseas

Your personal information is stored on Amazon Web Services infrastructure located in Sydney, Australia. Some of our service providers (for example, communications, support, analytics and security vendors) are located in, or may access information from, countries outside Australia, including the United States, the United Kingdom, the European Union, the Philippines and India. Before disclosing personal information to an overseas recipient, we take reasonable steps to ensure the recipient handles it in a way consistent with the APPs, either through contractual commitments or because the recipient is bound by a substantially similar privacy regime.

Where you have consented to a disclosure, or where the disclosure is required or authorised by Australian law, the additional accountability that APP 8.1 imposes on us may not apply. We will tell you, in a collection notice or in this policy, about any new categories of overseas recipient before we begin disclosing to them.

## 8. Data retention and deletion

We retain personal information only for as long as we need it for the purposes set out in this policy, or for as long as we are required to retain it by law. As a financial services provider, we are required by laws

including the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), the Corporations Act 2001 (Cth) and tax laws to retain certain transaction and identity records for up to seven years after the end of your relationship with us.

When personal information is no longer needed and we are not required to retain it, we will destroy it or de-identify it as soon as reasonably practicable. You can ask us to delete your personal information at any time using the contact details in section 14; we will tell you what we can delete, what we are required to keep, and for how long.

## 9. How we protect personal information

We take reasonable steps to protect personal information from misuse, interference, loss, and unauthorised access, modification or disclosure. Those reasonable steps include both technical and organisational measures, consistent with APP 11.3 as amended by the Privacy and Other Legislation Amendment Act 2024.

Our technical measures include:

- Encryption of personal information in transit (TLS) and at rest;
- Hosting on Amazon Web Services infrastructure in Sydney, Australia, with the security controls described at <https://aws.amazon.com/compliance/data-center/controls/>;
- Multi-factor authentication and least-privilege access controls for staff;
- Logging, monitoring and alerting for unauthorised or unusual access;
- Regular vulnerability scanning and security testing of our applications.

Our organisational measures include:

- Privacy and information-security training for staff;
- Documented information-security policies, incident response and data-breach response procedures;
- Contractual privacy and security obligations on our service providers;
- Periodic review of our security controls against current threats and good industry practice.

Despite these measures, no system is impenetrable. If a data breach occurs, we will respond in accordance with our internal data-breach response plan and our obligations under the Notifiable Data Breaches scheme described in section 10.

## 10. Notifiable data breaches

Paytime is bound by the Notifiable Data Breaches (NDB) scheme in Part IIIC of the Privacy Act 1988 (Cth). The scheme applies to all APP entities, including Paytime as a financial services provider.

If we have reasonable grounds to suspect that an eligible data breach has occurred – that is, an unauthorised access to, unauthorised disclosure of, or loss of personal information held by Paytime that is likely to result in serious harm to one or more individuals – we will:

- Promptly contain the incident and take steps to mitigate the risk of serious harm;

- Assess the suspected breach as soon as practicable, and in any event within 30 days, as required by the Privacy Act;
- If we conclude that an eligible data breach has occurred, prepare a statement in the form required by section 26WK of the Privacy Act and notify the Office of the Australian Information Commissioner (OAIC) as soon as practicable;
- Notify each affected individual as soon as practicable, by the method we ordinarily use to communicate with them (or, if that is not practicable, by any other reasonable means);
- Where it is not practicable to notify each affected individual directly, publish the statement on our Website and take reasonable steps to publicise its contents.

The notification will include our name and contact details, a description of the breach, the kinds of personal information involved, and the steps we recommend you take in response. You can read more about the NDB scheme on the OAIC website at [oaic.gov.au/privacy/notifiable-data-breaches](https://oaic.gov.au/privacy/notifiable-data-breaches).

## 11. Your privacy rights

### 11.1 How to make a request

You can ask us, at any time, to give you access to the personal information we hold about you, to correct it, or to delete it. You do not need to use any particular form, but giving us the following information helps us respond quickly:

- Your full name and the email address or phone number associated with your Paytime account;
- A brief description of what you are asking for (for example, “a copy of all my information” or “please correct my address”);
- Where relevant, the corrected information or the specific records you are interested in.

We may need to verify your identity before we act on the request, particularly for access and deletion requests. We will use the least intrusive method of verification reasonably available.

### 11.2 How to send the request

**Email:** [info@paytime.com.au](mailto:info@paytime.com.au) (preferred)

**Phone:** 1300 80 49 60 (Australia)

**Post:** Privacy Officer, Paytime Services Pty Ltd, PO Box H317, Australia Square NSW 1215

Our Privacy Officer is responsible for responding to privacy requests and complaints. Please put “Privacy request” in the subject line of any email so it is routed to the right place.

### 11.3 What you can ask for, and how we respond

What you can ask for	How we will respond
A copy of the personal information we hold about you (APP 12)	We will acknowledge your request within 7 days and give you access within 30 days of receiving enough information to identify you. We will not charge you to make the request. If we charge to give you access (for example, where the volume of information makes this necessary), the

What you can ask for	How we will respond
	charge will be reasonable and we will tell you what it will be before we incur it.
Correction of personal information that is inaccurate, out of date, incomplete, irrelevant or misleading (APP 13)	We will acknowledge your request within 7 days and correct the information, free of charge, within 30 days. If we have disclosed the incorrect information to a third party (e.g. your employer), we will, on your request, take reasonable steps to notify them of the correction.
Deletion of your personal information	We will delete or de-identify your personal information when it is no longer needed for any purpose described in this policy, unless we are required by law to retain it (for example, transaction records retained under tax or AML/CTF laws). You can ask us to delete your data at any time; we will tell you what we are able to delete and what we are required to keep, and why.
A statement attached to your record if we refuse to correct your information	If we do not agree that the information should be corrected, we will tell you why in writing. On your request, we will associate a statement with the information noting that you consider it to be inaccurate, out of date, incomplete, irrelevant or misleading.
A refusal explained	If we refuse access or correction, we will give you written reasons (except where giving reasons would itself be unreasonable), and tell you how to complain.

#### 11.4 If you are not satisfied – our complaints process

If you think we have breached the Privacy Act or the APPs, or you are unhappy with how we have handled your personal information, please tell us. Email your complaint to [info@paytime.com.au](mailto:info@paytime.com.au) or write to the Privacy Officer at the postal address above. Our process is:

- We will acknowledge your complaint in writing within 7 days of receipt.
- We will investigate and respond substantively within 30 days. If we need longer because the complaint is complex, we will tell you why and give you a revised timeframe.
- If our response does not resolve your concerns, you can ask us to escalate the matter within Paytime and we will arrange for a senior reviewer to consider it.

If you are still not satisfied, you can complain to the Office of the Australian Information Commissioner (OAIC):

- Website: [oaic.gov.au/privacy/privacy-complaints](https://oaic.gov.au/privacy/privacy-complaints)
- Phone: 1300 363 992
- Post: GPO Box 5288, Sydney NSW 2001

#### 11.5 Other avenues

Since 10 June 2025, individuals also have a statutory cause of action for serious invasions of privacy under Schedule 2 to the Privacy Act. This is a separate right that you may be able to enforce in court, in addition

to the OAIC complaints process. We mention it here for completeness; we encourage you to raise concerns with us first so we have an opportunity to put things right.

## 12. Marketing communications

We may send you marketing material about Paytime products, and the products of our Partners, using the contact details you have provided. You can opt out at any time by using the “unsubscribe” link in the message, updating your marketing preferences in your Paytime account, or contacting us at [support@paytime.com.au](mailto:support@paytime.com.au). We will action electronic marketing opt-outs within 5 business days and other marketing requests within 30 days. Even after you opt out, we will still send you transactional and service messages (for example, payment confirmations, security alerts and important account notices).

## 13. Cookies and online tracking

When you visit our Websites or use Paytime Services, we and our service providers place cookies, pixels, local storage and similar technologies on your device. We use them to keep you signed in, remember your preferences, secure the Websites against fraud, measure how the Websites are used, and – where you have not opted out – deliver marketing that is relevant to you.

We use Google Analytics and may use other analytics providers. We do not share information that directly identifies you with Google or other analytics providers. You can control cookies through your browser settings or through any in-product cookie controls we provide. Blocking cookies may affect the functionality of the Websites.

Most browsers offer a “Do Not Track” signal. The interpretation of that signal across the industry is not uniform; we currently do not respond differently to “Do Not Track” signals, but we treat the opt-out controls described above as effective expressions of your preference.

## 14. Contact us

Privacy Officer, Paytime Services Pty Ltd

Email: [info@paytime.com.au](mailto:info@paytime.com.au)

Phone: 1300 80 49 60 (Australia)

Post: PO Box H317, Australia Square NSW 1215

We aim to acknowledge all privacy-related enquiries within 7 days.