

Privacy Policy: AP+ and related entities

October 2025

CONTENTS

1. Applicability and entities	2
2. Personal information	2
3. Types of personal information we collect and hold	2
4. How we collect and hold personal information	4
5. Purposes for which we hold, use and disclose personal information.....	4
6. Technical & organisational measures	6
7. Access and correction	7
8. Overseas disclosure	7
9. Changes to this Privacy Policy	8
10. Complaints	8

1. Applicability and entities

- 1.1 Australian Payments Plus Ltd (ABN 19 649 744 203) (**AP+**), brings together, and is the holding company of Australia's three domestic payment providers; BPAY, eftpos and NPPA. This privacy policy applies to AP+ in addition to such payment providers and entities as follows:
- (a) BPAY Group Holding Pty Ltd (ABN 44 626 481 525) - which consists of BPAY Group Pty Ltd (ABN 60 003 311 644) and BPAY Pty Ltd (ABN 69 079 137 518) - manages the BPAY® bill payment service which allows customers to make bill payments through their financial institutions online banking service or via BPAY View and Osko®, a real time payments service that allows users to transfer funds to and from their accounts. Osko leverages the New Payments Platform which is infrastructure provided by NPP Australia Limited. Together, the BPAY entities are referred to as **BPAY**.
 - (b) eftpos Payments Australia Limited (ABN 37 136 180 366) operates the eftpos payment system, which is both a debit card payment system and a prepaid card payment system, Beem which provides a peer-to-peer payments facility/mobile application and ConnectID, a digital identity solution (**eftpos**).
 - (c) NPP Australia Limited (ABN 68 601 428 737) operates and manages the real-time account to account payments infrastructure in Australia (**NPPA**).
- 1.2 eftpos also owns and operates ConnectID, a digital identity exchange for identity verification. ConnectID is a separate initiative and has its own privacy policy. If you're engaging with ConnectID, please refer to the [ConnectID Privacy Policy- ConnectID](#).
- 1.3 eftpos also owns and operates Beem, a peer-to-peer payments facility. If you're engaging with Beem, please refer to the [Beem Privacy Policy](#).
- 1.4 Together, AP+, BPAY, eftpos and NPPA are referred to as **we, us, our**, throughout this privacy policy. In the course of carrying out each entity's activities, including providing each entity's services, websites, platforms, (together, the **services**), we will collect, store, use and disclose personal information. The collection, use and disclosure of your personal information may differ depending on which entity you engage with. This policy includes the types of personal information collected and held, and the purposes for which such information is used, by all entities generally as well as types and purposes specific to individual entities.
- 1.5 We are committed to the protection of your personal information and to compliance with applicable privacy laws.

2. Personal information

- 2.1 Personal information and/or personal data (the terms commonly used in applicable privacy laws), is information or an opinion about an identified or reasonably identifiable individual, whether or not the information or opinion is true and whether or not the information is recorded in a material form.

3. Types of personal information we collect and hold

- 3.1 We collect and hold personal information about individuals for the provision of the services and purposes connected to those services.

- 3.2 The types of personal information we may collect and hold differs depending on your interactions with the above entities. All entities may, from time to time, collect the following information about you.
- (a) *Identity and contact details* – including individuals’ full name, gender, address, date of birth, age, telephone number, email address and other contact information and identification information including driver’s licence, Medicare card, Australian passport, ID card issued by a foreign government, personal TFN or birth certificate.
 - (b) *Financial information* – bank and cheque account details, information associated with your payment and card details, including (if applicable) digital wallet details, details about your financial institution and your service providers.
 - (c) *Digital information* – text of written and oral communications gathered in the course of our interaction with you, including where you comment within our platforms and/or otherwise interact on live-chat, social media and emails, including feedback and online reviews and other information from your interactions with us online, including cookie information, IP address, URL’s, search histories and other associated information.
 - (d) *Other information for recruitment related activities* – if you apply for employment with us, employment history and related records, skills and experience, superannuation records, tax information including TFN according to legal requirements information about your personality, preference data.
- 3.3 In addition to the above types of personal information, some of our entities collect other types of personal information specific to, and necessary for, the activities and functions associated with providing their respective services. We set out these types of information specific to each entities’ activities and functions in the table below.

Entity	Types of personal information
AP+	We may also collect information about your opinions, policies, statement and writings.
eftpos	<p>We may also collect personal information in the following circumstances:</p> <ul style="list-style-type: none"> (a) <i>For business interactions</i>: the company you work for, business address, fixed line or mobile phone number, email address and social media and for sole traders, billing and bank account details. (b) <i>For certification authority services</i>: place of work, identification information. (c) <i>For payment processing</i>: device ID, location details, card details at the time of provisioning a card for mobile payments (this information is deleted as soon as practicable after provisioning, save for the tokenised card and device ID details which are de-identified), payment recipient information, user verification for card not present transactions and other device specific data and geolocation data at the time of use and card number.
BPAY	We may also collect information about your financial institutions and service providers.

4. How we collect and hold personal information

4.1 Across all entities, we may collect personal information as follows.

- (a) Directly from you, including in the course of providing our services and/or when you visit our websites and other online platforms and applications, including through the use of cookies (data files placed on your device or computer).
- (b) From third parties where it is unreasonable or impractical to collect the information directly from you, for example, from banks, retailers, merchants, payment service providers and payment processors that make up AP+'s member-owned organisation (**Users**), from our subsidiaries, and from other entities that provide payment processing, disputes, chargeback handling and related services.
- (c) From publicly available sources of information, such as social media.

4.2 In relation to BPAY, there are additional ways that we may collect personal information from you, which we set out here.

- (a) If you or your organisation elects to subscribe to one of BPAY's scheme products offered under a payment scheme (i.e. BPAY Payments and Osko), we may receive a range of personal information about you either:
 - (i) directly from you through the BPAY operations portal or other means such as email; or
 - (ii) indirectly from third parties including your financial institution or your service providers, in the course of managing transactions and conducting investigations and adjustments (for example investigating disputes, mistaken payments, fraud, etc.).
- (b) If you use any product or service we may offer in connection with one of BPAY's scheme products offered under a payment scheme, for example by registering as a user or developer for our APIs, we may receive personal information provided by you in connection with such use.

4.3 Personal information is held securely, is subject to various security protections and is held only for as long as the information remains relevant to the purpose for which it was collected, and in accordance with our business needs and legal requirements.

4.4 We will destroy or permanently de-identify your personal information we are holding when it is no longer needed for the purpose for which we collected it. When we destroy your personal information, we will ensure that this is carried out properly and securely.

5. Purposes for which we hold, use and disclose personal information

5.1 We will not use or disclose personal information for any secondary purpose, unless that secondary purpose is related to the primary purpose for which we have collected that information, and you would reasonably expect the disclosure in the circumstances, or unless you consent to that use or disclosure. While you are under no obligation to provide us with your personal information, unfortunately we may

not be able to provide you with the products, services or information which you require if you do not provide us with:

- (a) all the personal information we ask for; or
- (b) consent to disclose that information to other entities, our service providers or third parties as described in this Privacy Policy.

AP+ cannot provide products, services or information to you if you wish to remain anonymous or use pseudonymous.

5.2 All entities may, from time to time, use your personal information for the following purposes:

- (a) conducting our business and functions, which includes providing and designing our services, or providing the services of a third party, to you;
- (b) to communicate information about our products or services or third party products or services we believe may be of interest to you;
- (c) where you have consented, to provide you with information or advertising relating to our products or services (including targeted advertisements) or marketing communications we believe may be of interest to you;
- (d) to match transactions data to combat fraud and investigate suspicious or fraudulent activity;
- (e) to improve the products and services of each entity and provide de-identified and aggregated demographic and behavioural insights to third parties such as merchants with whom a group entity is associated;
- (f) for the purposes of collaborating on projects in respect of our products and services with our subsidiaries and counterparts;
- (g) for our internal administrative, research, planning, marketing and product development purposes; and
- (h) to comply with legal obligations.

5.3 In addition to the above purposes, the purposes for collection, storage and disclosure will differ depending on the ways in which each of our entities need to use such information to provide their respective services. We set out some specific purposes in the table below.

Entity	Specific purposes for collecting, holding, using and disclosing personal information
AP+	AP+ may also use your personal information to perform its functions as holding company and facilitate communication between Users.
NPPA	NPPA may also use your personal information to facilitate communication between Users.
eftpos	eftpos may also use your personal information to: <ul style="list-style-type: none"> (a) verify your identity (e.g. for certification authority services or for marketing competition winners);

	<p>(b) provide you or, where you work for an eftpos member or participant entity or partner counterparty, your employing entity, with documents and information relevant to your or your entity's participation in any of the eftpos payment system, Beem or the ConnectID digital identity scheme; and</p> <p>(c) attend to matters relating to product provisioning, loyalty program support, business analysis or dispute resolution.</p>
--	--

5.4 All entities may disclose personal information to:

- (a) Users;
- (b) parent companies and other affiliates and related bodies corporate;
- (c) government and law enforcement agencies where we are required or authorised to do so by law, including in response to a lawful request by any government, regulatory body or enforcement agency;
- (d) service providers, but only for the purpose of providing goods or services to us, including direct marketing and communication agencies, identification verification agencies and entities that help us meet our regulatory compliance obligations; and
- (e) to entities involved in connection with a corporate merger, consolidation, restructuring, the sale of substantially all of our interests and/or assets, or other corporate change requiring the transfer of assets, including during the course of any due diligence process, to the purchaser or surviving entity.

5.5 In relation to eftpos, there are additional entities to whom we might disclose your personal information, which we set out here:

- (a) eftpos payment system members (which are banks, independent acquirers and retailers and their aggregator service providers), as necessary, to enable us to provide any of our products or services to you or answer enquiries and administer governance activities related to our rules; and
- (b) participants in the digital identity broker solution for the purposes you have authorised them to seek or provide your personal information.

5.6 We may also disclose personal information to third party partners and organisations (including partners and organisations who we engage to assist us in providing our services), third party technology and marketing partners (including Amazon Web Services, Facebook marketing services and Google Analytics) and other technology and marketing service providers for their use for the same purposes.

6. Technical & organisational measures

6.1 We take reasonable steps, including both technical and organisational measures, to protect and safeguard your personal information.

6.2 Technical measures include, but are not limited to:

- (c) Encryption;

- (d) Secure system controls (including role-based permissions, configuration, authentication and access management); and
- (e) Regular system testing.

6.3 Organisational measures include, but are not limited to:

- (a) Employee training & awareness initiatives;
- (b) Information security and data protection policies and procedures;
- (c) Third party risk assessments & risk management programs; and
- (d) Business continuity and disaster recovery planning.

6.4 Our technical and organisational measures are subject to ongoing review and may be updated from time to time (and more frequently than this Privacy Policy is reviewed and updated), to reflect changes in technology, legal obligations or business requirements.

7. Access and correction

- 7.1 We will take all reasonable steps to ensure any personal information we collect, use or disclose is up to date and accurate. If you believe personal information that we hold about you is not up to date or accurate, you may ask us to correct it.
- 7.2 You may ask us to provide you with details of the personal information we hold about you, and copies of that information. We will respond to your request and attempt to provide you with the relevant information within 30 days of receipt of your request.
- 7.3 If we provide you with copies of the information you have requested, to the extent permitted by law, we may charge you a reasonable fee to cover the administrative costs of providing you with that information.
- 7.4 Please direct all requests for access and correction to privacy@auspayplus.com.au

8. Overseas disclosure

- 8.1 Our group entities may, in the course of providing their respective products and services, disclose personal information overseas, including to services providers, processing agents or third parties who store data or operate outside Australia.
- 8.2 Those entities store data or operate in countries including but not limited to the United States of America, Singapore, the United Kingdom, Ireland, Germany, Japan.
- 8.3 Regardless of the location of data storage or processing, we will impose adequate data protection safeguards and implement appropriate measures to ensure that your personal data is protected in accordance with applicable data protection laws.

9. Changes to this Privacy Policy

- 8.1 We will review this Privacy Policy at least once every two years. We may update this Privacy Policy from time to time. We recommend that you review the terms of this policy periodically to make sure that you are aware of how we collect, hold, store and use personal information. The date this policy was last updated will be set out at the start of the policy.

10. Complaints

General

- 10.1 If you consider a breach of the Privacy Act 1988 (Cth) has occurred, you may direct your query to our privacy officer at privacy@auspayplus.com.au and we will attempt to resolve your complaint.
- 10.2 If you do not consider our response satisfactory, you may contact the Australian Privacy Commissioner at its website www.oaic.gov.au or by telephone on 1300 363 992.
- 10.3 Some of the individual entities have additional mechanisms in respect of complaints. We set those out here.

AP+ or NPPA

- 10.4 AP+ and NPPA are unable to handle or assist you with a privacy complaint involving a financial institution which is an AP+ or NPPA Member. If you have a privacy complaint about an AP+ or NPPA Member, you should make your complaint directly to the organisation or financial institution concerned.

This policy supersedes any previous Privacy Policies adopted by an entity of the AP+ Group.