

Effective date | 16 April 2026

Data Handling and Electronic Verification Statement

Contents

Introduction	3
Why we collect information	3
How we collect your information	3
What personal information is collected?	3
What happens if I do not provide my information?	3
Electronic identity verification	4
Disclosing your personal information	4
Cross-border disclosures	4
Data aggregation	4
Security of your personal information	4
Updating your personal information	4
Our contact details	5
Complaints and feedback	5
More information on our Privacy Policy	5

Introduction

This statement covers MyState Bank and extends to its operational divisions, including Auswide Bank and Selfco. The use of we/us/our within this Policy refers to MyState Bank Limited and any entity owned or controlled by us.

MyState Bank collects and handles personal information as part of the provision of services to you, this can occur throughout your customer journey. From time to time you may be required to provide additional information.

As part of the provision of services we also undertake electronic identity verification to help confirm who you are.

We are bound by the Privacy Act 1988 (Cth) and we are committed to respecting and protecting your personal information.

This statement explains how we collect, hold, use and disclose your personal information for these services.

Why we collect information

We collect personal information to open and manage your accounts, provide you with services, verify and authenticate your identity, prevent fraud, communicate with you, operate and improve our services, and meet our legal obligations. In some cases, we are required or authorised by law (for example, under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) to collect certain information. Collection of information can occur throughout your customer journey.

How we collect your information

We will usually collect information directly from you (e.g. during digital onboarding, account opening, and account servicing).

Sometimes we may also collect information from reliable and independent sources such as, but not limited to a credit reporting agency or government agency to verify your identity, or from third parties you authorise (e.g. an identity service provider such as DVS).

If you are already a customer of MyState Bank, we may already hold information about you and have identified you. If so, we may use the information we already hold and where permitted to do so by law.

What personal information is collected?

We only collect personal information about you that we reasonably need.

This may include, but is not limited to your:

- » name
- » date of birth
- » contact details
- » residential address
- » information supporting account set-up and servicing
- » government issued identifiers (e.g. driver licence or Medicare numbers) for lawful identity verification with the issuing authority
- » Biometric information used for identity verification only, (data is deleted after 30 days)
- » device information
- » other information we are required or authorised by law to collect.

Providing your Tax File Number (TFN) is optional. If provided, we handle TFNs in line with the Privacy (Tax File Number) Rule 2015 and tax laws. We do not use TFNs to verify identity or as our customer identifier.

When you seek financial assistance (hardship), we may also collect additional information you provide about your circumstances so we can assess your request.

This may include:

- » gender
- » employment status
- » income
- » expenditure
- » assets and liabilities
- » nature of financial distress

Where it is necessary to do so, we may collect personal information about you that is sensitive. Sensitive information includes information about an individual's health, and membership of a professional or trade association. Unless we are required or permitted by law to collect information, we will first obtain your consent.

What happens if I do not provide my information?

If you do not provide your personal information we request, we may not be able to verify your identity to open your account, or provide some services.

Electronic identity verification

Under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), we are required to verify your identity on application and at times throughout our relationship. For electronic verification, we may pass your details (for example, your name, address and date of birth, and details from your identity documents) to external organisations to verify your identity.

If you prefer not to use electronic verification, please contact us and we will offer a manual alternative (for example, presenting original or certified documents in branch).

The entities we use to help us can include (but are not limited to):

- » credit reporting bodies (for identity-match only, not a credit check)
- » government agencies (e.g. the Australian Government's Document Verification Service (DVS))
- » external data storage providers (e.g. Equifax Pty Ltd)
- » publicly available sources (such as White Pages)
- » official record-holders accessed via third-party systems.

It is an offence under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) to provide false or misleading information about your identity.

Disclosing your personal information

Personal information (including identity verification information) may be shared with our partners and service providers throughout the application and account servicing process. We explain how we verify your identity electronically in the "Electronic identity verification" section of this statement.

We may disclose personal information to:

- » identity verification service providers and accredited intermediaries
- » cloud hosting, data storage and platform providers
- » fraud prevention and cybersecurity service providers
- » customer support and communication service providers
- » professional advisers and auditors
- » law enforcement bodies, regulators and government agencies where required or authorised by law
- » members of our corporate group for the purposes described in this statement.

We require recipients to handle personal information consistently with this statement, our Privacy Policy and applicable laws.

Cross-border disclosures

Some suppliers or their sub processors may be located outside Australia. Likely overseas locations include:

- » United States
- » United Kingdom
- » Ireland
- » China
- » Canada
- » India
- » Philippines
- » New Zealand
- » Netherlands and
- » countries within the European Union.

Overseas disclosure occurs only where necessary for service provision and is subject to safeguards. Before any overseas disclosure, we take reasonable steps (for example, contractual, technical and organisational measures) to ensure the overseas recipient protects personal information in a manner substantially similar to the Australian Privacy Principles.

Data aggregation

We may de-identify and aggregate information we hold about you and other individuals by removing information that could identify you. We use anonymised data for internal purposes, e.g. service improvements and analytics, and we may share insights with third parties but not in a form that can re-identify you.

Security of your personal information

We take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. We restrict access on a need-to-know basis and securely destroy or de-identify your information when it is no longer needed.

Updating your personal information

You can request access to, or correction of, your personal information by contacting us on 138 001 or via email at privacy@mystate.com.au. You may also be able to update some details directly where available (for example, via 'My Profile' on a platform we provide).

Our contact details

If you have any questions or concerns about our Privacy Policy or our handling of your personal details please contact us.

Privacy Officer

Email: privacy@mystate.com.au

Post: GPO Box 1274, Hobart TAS 7001

Complaints and feedback

We take your feedback seriously and strive to address all concerns about your personal information. You can make a complaint or provide feedback by contacting us. We will acknowledge your complaint within 1 business day and aim to resolve it within 30 days. If your complaint relates to financial hardship or credit, we will respond within 21 days. If you wish to lodge a complaint please contact the specific entity the complaint relates to on the details below.

How can I lodge a complaint?

You can advise us of your complaint or provide feedback by:

MyState Bank:

Using the online form at mystate.com.au;

Phone: 138 001

Email: mycomplaint@mystate.com.au

Mail: Complaints and Feedback,
GPO Box 1274,
Hobart TAS 7001

Auswide Bank:

Using the online form at auswidebank.com.au

Phone: 1300 138 831

Email: customer@auswidebank.com.au

Mail: Complaints and Feedback,
Auswide Bank Ltd,
GPO Box 75, Brisbane QLD 4000

Selfco:

Phone: 1300 12 11 10

Email: leasing@selfco.com.au

Mail: Complaints and Feedback,
PO Box 7956,
Baulkham Hills BC NSW 1755

For further information on the MyState Bank complaints process please refer to the Complaints Policy located on the website.

Australian Financial Complaints Authority (AFCA)

Online: www.afca.org.au

Phone: 1800 931 678

Email: info@afca.org.au

Post: Australian Financial Complaints Authority GPO
Box 3, Melbourne VIC 3001

Office of the Australian Information Commissioner (OAIC)

Online: www.oaic.gov.au

Phone: 1300 363 992

Mail: OAIC - CDR Complaints GPO Box 5218, Sydney
NSW 2001

More information on our Privacy Policy

If you would like more information on how we use our information please see our full [privacy policy](#) available on our website.

