EUROPEAN UNION DATA PROTECTION

Privacy statement (National Australia Bank Europe S.A.)

541036-3-170-v1.0
© 2018 National Australia Bank Limited ABN 12 004 044 937 AFSL and Australian Credit Licence 230686 A143198-0518

Privacy statement

We respect your personal information, and this privacy notice explains how we handle it and your privacy rights. We take appropriate measures to ensure NAB can engage securely with and for our customers.

This notice was last updated in September 2026 and applies to National Australia Bank Europe S.A., which is established in France. We review it at least once a year, and the current version is always available at www.nabeurope.com.

In France, the GDPR is supplemented by Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties (the 'Loi Informatique et Libertés'), as amended. Where this notice refers to your rights, those rights arise under both the GDPR and that law, and in some cases French law gives you additional rights, which are explained below.

Scope

This notice applies to the collection and processing of your personal data if you are in a country that is a member of the European Economic Area (EEA). National Australia Bank Europe S.A. is the controller of that personal data. We are part of the National Australia Bank group of companies (the 'Group'), whose ultimate parent is National Australia Bank Limited, incorporated in Australia.
National Australia Bank Europe S.A. ('we', 'us', 'NAB Europe') is a société anonyme with its registered office at Level 3, 24 rue des Capucines, 75002 Paris, France. Other Group members act as controllers in their own right for their own processing and publish their own privacy notices. For further information about Group members see **www.nab.com.au.**

This notice tells you how we collect and process your personal information and the legal basis for processing it, what we use it for and who we share it with. It also explains particular rights you have in relation to the processing of your personal information.

We are grateful for the trust and confidence you have in us to safeguard your privacy.

Contact us

We care about your privacy and welcome your feedback. Please contact us if you have any questions or comments about this notice, our Group privacy policies, and procedures, or you wish to exercise the rights you have under applicable privacy laws, which are explained further below.

You can contact us by:

- using our feedback email address gdpr.nabeurope@eu.nabgroup.com

- **Office of the Group Data Protection Officer, and NAB's compliance with the EEA's GDPR**

NAB's Global Privacy Office and its Group Data Protection Officer monitor and advise on compliance with the global privacy laws including the EU General Data Protection Regulation 2016/679 (the 'GDPR') which applies to NAB when processing the personal information of individuals (data subjects) who are in countries in the EEA in relation to offering them NAB's products or services or monitoring their behaviour when in those countries.

The contact details of NAB's Global Privacy Office are as follows:

The Global Privacy Office,
National Australia Bank Limited
Level 1 800 Bourke Street,
Docklands
Melbourne
Victoria 3008 Australia.

Email: **global.privacy.office@nab.com.au**

As our main establishment in the EEA is in France, our lead supervisory authority is the French data protection authority, the Commission Nationale de l'Informatique et des Libertés ('CNIL').

Our Data Protection Officer is notified to the CNIL, as required by Article 37(7) of the GDPR.

Categories of personal data

The categories of information that we collect from other sources include:

- Identity verification (from government agencies, background checking companies) to protect you against fraud.

- Financial history (including becoming insolvent / bankrupt).

- Property information (in relation to loan applications, valuers, agents, referrers, brokers, mortgage managers, solicitors, conveyancers, and settlement agents).

We may also collect information about you when you communicate (including through emails or other messages) with one of our employees or other third parties who are using computers provided by NAB, including:

- we may monitor use of NAB devices for the purpose of ensuring that NAB employees comply with applicable laws and NAB's internal policies (including as part of internal and/or external investigations); and

- such monitoring may collect your personal information, including in the form of metadata from emails and messages (such as email subjects and the sender / recipient(s)). In very limited and specific scenarios (e.g., where there is suspicion of serious misconduct or a crime by a NAB employee), such monitoring may also collect and process your personal information through the recording / capture of the NAB

employee's device screen as part of the monitoring of that employee.

- Where this monitoring takes place in France, we also comply with French labour law. In particular, employees are informed individually before any monitoring is introduced, in accordance with Article L1222-4 of the Code du travail; the social and economic committee is consulted in accordance with Article L2312-38; and we carry out a data protection impact assessment under Article 35 of the GDPR before introducing any systematic monitoring. Capture of an employee's screen is used only in exceptional and documented circumstances, and is subject to specific internal authorisation.

Sources of personal data

Sometimes we collect information about you from other sources. We may collect information about you that is publicly available (for example from public registers or social media) or that is otherwise made available by third parties. For instance, we do this where:

- we distribute or arrange products on behalf of others, including our business partners.
- we can't get hold of you and need to update your contact details.
- we need information from third parties about an application you make through us.
- we need information for fraud detection and prevention purposes.
- we are checking the security you are offering.
- we can learn insights about your financial needs, such as through property information.
- you have consented to third parties sharing it with us, such as organisations we have loyalty programs with, or we sponsor.
- at your request, we exchange information with your legal or financial advisers or other representatives.

We may use or disclose information about you to combine the information that we hold with information collected from or held by external sources. We do this in order to enable the development of customer insights about you so that we can serve you better. This includes being able to better understand your preferences and interests, personalise your experience, enhance the products and services you receive, and to tell you about products and services that may be of interest to you.

How we use and process the personal information we collect about you We may use and process your information to:

- perform our contract with you (or the entity you represent) and respond to your related requests.
- provide you with the product or service you asked or applied for, or in order to respond to your request before we provide the product or service (e.g., checking your information with others on your request) including to give you information about the product or service including financial help, guidance, and advice.
- consider whether you are eligible for a product or service you have asked for, including identifying or verifying you or your authority to act on behalf of a customer;
- process your application and provide you (or the entity you represent) with a product or service;
- administer the product or service we provide you, which includes answering your requests and complaints, varying products and services, and managing our relevant product portfolios;
- determine whether a beneficiary will be paid a benefit.

In connection with our legitimate interests in carrying on our business

We may use your information for our legitimate interests (where we consider these are not overridden by your rights noting that you have the right to object to as explained below) in:

- identifying opportunities to improve our service to you and improving our service to you.
- conducting market research to serve you better by understanding your preferences to ensure we send you appropriate promotions and campaigns.
- assisting in arrangements with other organisations (such as loyalty program partners) in relation to a product or service we make available to you.
- allowing us to run our business and perform administrative and operational tasks (such as training staff, risk management, developing and marketing products and services, undertaking planning, research and statistical analysis, and systems development and testing).
- verifying identity, maintaining, or improving security, preventing, or investigating any fraud or crime, or any suspected fraud or crime (including the collection of any of your personal information incidentally as part of our employee surveillance and monitoring program).

Under a legal obligation

We may also use and process your personal information where we are required by applicable laws, regulations or codes that bind us, in particular

© 2026 National Australia Bank Europe S.A.

as a financial institution. These include company and tax law and anti-money laundering law which, among other things, require us to verify your identity.

For NAB Europe, these obligations arise principally under French and European Union law. They include Articles L561-1 and following of the Code monétaire et financier on customer due diligence and anti-money laundering, the tax identification and reporting obligations that apply to French financial institutions, and European Union restrictive measures (sanctions).

We also operate an internal whistleblowing channel in accordance with Law No. 2016-1691 (Sapin II), as amended by Law No. 2022-401. Where personal data is contained in a report, we handle it confidentially, restrict access to it, and follow CNIL guidance on the management of whistleblowing schemes.

With your consent

Where required under the GDPR (as relevant), we will use your personal information for the purpose for which you have given your valid or explicit consent for. We will ensure we have obtained your consent if it is required before we process your information.

For example, some information you provide us in connection with your application for or the administering of a product or service we provide you, may be more sensitive and therefore falls within a special category of personal information, such as health information. We will collect and process this information only with your explicit consent.

For direct marketing

With your consent where it is required by law, we may communicate with you (through the preferred communication channel(s) you have selected, which may include by email, telephone, SMS, iM,

mail, or any other electronic means including via social networking forums) to:

- tell you about **other NAB Group** products, services and offers that may be of interest to you.
- run competitions and other promotions.

If you have provided your consent to receive direct marketing, you can withdraw it at any time without detriment, we will process your request as soon as practicable.

In France, marketing by email, SMS and other electronic means is subject to Article L34-5 of the Code des postes et des communications électroniques. This requires your prior consent where you are contacted as an individual consumer, but allows us to contact you without consent where you are contacted in a professional capacity about a product or service relevant to your role.

The rules on marketing by telephone in France changed on 11 August 2026. Under Law No. 2025-594 of 30 June 2025 and Decree No. 2026-662 of 23 July 2026, we may only telephone a consumer for marketing purposes where that person has given prior consent by a clear positive act, or where the call relates to an existing contract and concerns the subject matter of that contract. A pre-ticked box or a clause buried in general terms is not valid consent. The Bloctel opposition list ceased to operate on that date.

Consent to telephone marketing lasts for no more than one year and is not tacitly renewed. You can withdraw it at any time and by simple means, including orally during a call, and we will act on your withdrawal without charge.

Where you have subscribed to something specific (like hearing from one of our sponsored organisations) then these subscriptions will be managed separately. If you no longer wish to receive these emails, you can use the unsubscribe option in any message we send you, or contact us using the details in ‘Contact Us’. You do not need to log in to any service to opt out.

Where you have subscribed to something specific (like hearing from one of our sponsored organisations) then these subscriptions will be managed separately. If you no longer wish to receive these emails you may log into Internet Banking and update your preferences.

How we use your credit information In addition to the basis on which we use and process your personal information described above, we may also use and process your credit information (which may be for our legitimate interest, or with your consent or to perform a contract we have with you) to:

- enable a mortgage insurer or title insurer to assess the risk of providing insurance to us or to address our contractual arrangements with the insurer.
- assess whether to accept a guarantor or the risk of a guarantor being unable to meet their obligations.
- consider hardship requests.
- assess whether to securitise loans and to arrange the securitising of loans.
- Where we assess creditworthiness in France, we may consult the registers maintained by the Banque de France, including the Fichier national des incidents de remboursement des crédits aux particuliers (FICP) and the Fichier central des chèques (FCC), where we are entitled to do so. Information held in those registers is corrected through the Banque de France's own procedure, and we will tell you how to use it if that is the right route for your request.

- In line with CNIL guidance on assessing solvency in the granting of credit, we apply the following limits. Where you are not already a customer and we decline your application, we keep your application data in active use for no more than six months from the date of the application, and use it only to assess that application and any further credit application you make; after that it is held in intermediate archive for evidential purposes only, for the applicable limitation period. Information about a payment default is used to assess creditworthiness for no more than twenty-four months after the default has been fully regularised, judged against how serious the incident was. Where you have completed an over-indebtedness (surendettement) procedure, we will stop using that information to assess your creditworthiness once the procedure is complete and the debt has been settled in accordance with it.

Cookies and other trackers

When you visit our websites or use our digital channels, we and our partners may place cookies and similar trackers on your device, or read information already stored on it. In France this is governed by Article 82 of the Loi Informatique et Libertés, which implements the ePrivacy Directive, and is enforced by the CNIL.

We place trackers that are strictly necessary to provide a service you have asked for, or to keep your session secure, without asking you. For all other trackers, including those used for audience measurement and advertising, we ask for your consent first. Refusing is as simple and as quick as accepting, refusing does not prevent you from using our website, and you can change your choice at any time through the cookie settings on our site.

In line with CNIL guidance, our trackers have a lifetime of no more than thirteen months and are not automatically extended when you visit again; once that period expires we ask for your consent again. We keep a record of your choice, including a refusal, so that we do not have to ask you on every visit. Details of the trackers we use, their purposes and their lifetimes are set out in our cookie notice.

When the law authorises or requires us to collect information

We may collect information about you via application forms, online, or in person, because we are required or authorised by law to collect it, or where a contractual requirement exists, or the collection is necessary in order to enter into a contract with you.

There are laws that affect financial institutions, including company and tax law which require us to collect personal information.

For example, we require personal information to verify your identity under applicable local AntiMoney Laundering law.

© 2026 National Australia Bank Europe S.A.

What happens if you don't provide your information to us?

If you don't provide your information to us, we may not be able to:

- provide you (or the entity you represent) with the product or service you want.
- respond to your requests.
- manage or administer your product or service.
- personalise your experience with us.
- verify your identity or protect against fraud; or
- let you know about other products or services from our Group that might better meet your financial, e-commerce and lifestyle needs.

You have the right not to be subject to a decision by NAB made solely by automated processing. NAB may use automated processing (including profiling) but does not make decisions about you only on this basis.

Sharing your information We may share your information with other organisations consistent with the purposes for which we use and process your information as described above. This includes with the entities described below.

Sharing with the Group

We may share your personal information with other Group members. This could depend on the product or service you have applied for and the Group member you are dealing with. Where appropriate we integrate the information, we hold across the Group to provide us with a complete understanding of you and your needs in connection with the product or services we are providing you, including giving you access to the Group or related products you hold via Internet Banking.

We may also share your personal information with other Group members where it is necessary to do so as part of the employee surveillance and monitoring program. This may involve transfer of your personal data outside the EEA, including to Australia, in which case we will ensure that the relevant protections are put in place prior to such transfer.

Sharing at your request

At your request, we will share your personal information with your representative or any person acting on your behalf (for example, financial advisers, lawyers, settlement agents, accountants, executors, administrators, trustees, guardians, brokers, or auditors) and your referee.

Sharing with third parties

We may disclose your personal information to third parties outside of the Group including to help us run

our business operations, locations, and sites, many of whom are based outside EEA with the majority based in Australia. These third parties include:

- those involved in providing, managing, or administering your product or service.
- authorised representatives of the NAB Group who sell products or services on our behalf.
- credit reporting bodies or other approved third parties who are authorised to assess the validity of identification information.
- insurance, investment, superannuation and managed funds organisations, and their advisers and service provider.
- medical professionals, medical facilities or health authorities who verify any health information you may provide where necessary for insurance purposes.
- real estate agents, valuers, and insurers (including lenders' mortgage insurers and title insurers), re-insurers, claim assessors and investigators.
- brokers or referrers who refer your application or business to us.
- other financial institutions, such as banks, as well as guarantors and prospective guarantors of your facility.
- organisations involved in debt collecting, including purchasers of debt.
- fraud reporting agencies (including organisations that assist with fraud investigations and organisations established to identify, investigate and/or prevent any fraud, suspected fraud, crime, suspected crime, or misconduct of a serious nature).
- organisations involved in surveying or registering a security property, or which otherwise have an interest in such property.
- organisations we sponsor and loyalty program partners, including organisations the NAB Group has an arrangement with to jointly offer products or has an alliance with to share information for marketing purposes.
- companies we arrange or distribute products for, such as insurance products.
- rating agencies to the extent necessary to allow the rating agency to rate particular investments.
- any party involved in securitising your facility, (sometimes this information is de-identified),
- reinsurers and underwriters, loan servicers, trust managers, trustees, and security trustees.
- service providers that maintain, review, and develop our business systems, procedures,
- and technology infrastructure, including testing or upgrading our computer systems.
- payments systems organisations including merchants, payment organisations and organisations that produce cards, cheque books or statements for us.
- our joint venture partners that conduct business with us.
- organisations involved in a corporate reorganisation or transfer of NAB Group assets or business.
- organisations that assist with our product planning, analytics, research, and development.
- mailing houses and telemarketing agencies and media organisations who assist us to communicate with you including for direct marketing purposes with your consent, including media or social networking sites.
- other organisations involved in our normal business practices, including our agents and contractors, as well as our accountants, auditors or lawyers and other external advisers (e.g., consultants and any independent customer advocates); and
- government or regulatory bodies as required or authorised by law (in some instances these bodies may share it with relevant foreign authorities).

Sharing with other Organisations

We may need to share some of the information we collect about you from the EEA with organisations both inside and outside Australia, sometimes we may need to ask you before this happens.

You can view a list of the countries in which those overseas organisations are located at **www.nab.com.au/privacy/overseas-countrieslist/**.

We may store your information in cloud or other types of networked or electronic storage. If your information is stored in this way, disclosures may occur in countries other than those listed.

We are a global business, headquartered in Australia, with operations and service providers in a number of countries outside the EEA, including Australia and India. Where we transfer your personal data outside the EEA, we do so on the basis of one of the following: an adequacy decision of the European Commission covering the country concerned; the standard contractual clauses adopted by the European Commission in Implementing Decision (EU) 2021/914, together with an assessment of the laws of the destination

country and any additional measures that assessment shows are needed; or, in limited cases, a derogation permitted by Article 49 of the GDPR.

Overseas organisations may be required to disclose information we share with them under an applicable foreign law.

What happens when we no longer need your information?

We'll only keep your information for as long as we require it for our purposes. We're required to keep some of your information for certain periods of time under law, such as the Corporations Act, the Anti-Money Laundering & Counter-Terrorism Financing Act, and the Financial Transaction Reports Act for example. When we no longer require your information, we'll take steps to ensure that your information is destroyed or deidentified.

We are required to keep your information for 7 years from the closure of accounts, or 10 years from the termination of superannuation facilities, or otherwise as required for our business operations or by applicable local laws.

We may need to retain certain personal information after we cease providing you with products or services to enforce our terms, for fraud prevention, to identify, issue or resolve legal claims and/or for proper record keeping.

We may also retain a record of any stated objection by you to receiving Group marketing for the purpose of ensuring we can continue to respect your wishes and not contact you further.

Your personal information rights

How to access your information Subject to applicable laws, you have the right to access your personal information and to receive a copy of that information.

You can ask us to access your personal information by emailing **gdpr.nabeurope@eu.nabgroup.com**

You can also ask that personal information provided by you to us is transmitted to another party.

We may need to verify your identity to respond to your request. We will respond to any request within a reasonable period permitted under applicable privacy laws and will generally give access unless an exemption applies to certain information.

We will give you access to your information in the form you want it where it's reasonable and practical. We may charge you a small fee under certain circumstances to cover our costs when giving you access but we'll always confirm this with you first.

If we can't give you access, we will tell you why in writing and how you can make a complaint about our decision.

If you have concerns, you can complain. See 'Contact Us'.

How to correct your personal information You have the right to correction (rectification) of personal information and can contact us if you think there is something wrong with the information, we hold about you.

If you are worried that we have given incorrect information to others, we will tell them about the correction. If we can't, then we'll let you know in writing.

Your right to erasure of your information

You also have in certain circumstances the right to request that the personal information that NAB collects from you is erased. If we refuse any request you make in relation to this right, we will tell you why in writing and how you can make a complaint about our decision.

Your right to object to or restrict processing of your information

You may also request that further processing of your personal information is restricted in certain circumstances, including while we investigate your concerns with this information.

How to access your credit eligibility information

Where you request access to credit information that NAB obtained from credit reporting bodies or which it based on that information, we will:

- provide you access to the information within 30 days (unless unusual circumstances apply); and
- ask you to check with credit reporting bodies what information they hold about you to ensure it is accurate and up to date. If we can't give you access, we will tell you why in writing and how you can make a complaint about our decision. If you have concerns, you can complain to the Australian Information Commissioner or the French Commission Nationale de l'Informatique et des Libertés.

Correcting your credit information Whether we made the mistake or someone else made it, we are required to help you correct the information within 30 days. If we can't make a correction in that timeframe, we will ask you for extra time. We also might need to talk to others in order to process your request. The most efficient way for you to make a correction request is to ask the organisation which made the mistake.

Whether we're able to correct the information or not, we'll let you know within five business days of deciding to do this. If we can't we will provide reasons. We'll also let the relevant third parties

© 2026 National Australia Bank Europe S.A.

know as well as any others you tell us about. If there are any instances where we can't do this, then we'll let you know in writing. If you have any concerns, you can make a complaint to the Australian Information Commissioner or the French Commission Nationale de l'Informatique et des Libertés.

Right to object to data processing and right to data portability

You also have in certain circumstances the right to request that the further processing of your information is restricted or to object to its processing and the right to data portability (to receive and have transferred the information you provided). If we refuse any request you make in relation to this right, we will write to you to explain why and how you can make a complaint about our decision.

Right to withdraw consent

You can let us know at any time if you no longer wish to receive direct marketing updates from the Group. We will process your request as soon as practicable. Where you have subscribed to something specific (like to hear from one of our sponsored organisations) then these subscriptions will be managed separately.

What happens to your personal data if you die

You may also withdraw your consent where provided or object to the further processing of your personal information under certain circumstances. If we refuse any request you make in relation to this right, we will write to you to explain why and how you can make a complaint about our decision.

The withdrawal of your consent will not affect the processing of your information that you had consented to.

French law gives you rights over what happens to your personal data after your death. These are set out in Articles 84 to 86 of the Loi Informatique et Libertés and they have no direct equivalent in the GDPR.

You can give directives about the retention, erasure and disclosure of your personal data after your death. General directives can be registered with a certified trusted third party. Directives that relate specifically to the personal data we hold can be registered with us, and you can appoint a person to carry them out. You can change or withdraw your directives at any time, and any contractual term that seeks to limit these rights is treated as void under French law.

If you have not left directives, your heirs may, on proof of their identity and status, exercise certain rights: they may access your personal data to the extent needed to organise and settle your estate, ask us to close your accounts, object to our continuing to process your personal data, and ask us to update our records to take account of your death. If they ask us to, we will confirm free of charge that we have done what was requested.

These rights do not override obligations that require us to keep certain records, or the duty of banking secrecy that we owe in respect of other people.

How do you make a complaint? If you have a complaint about how we handle your personal information, we want to hear from you. You are always welcome to contact us. We are committed to resolving your complaint and doing the right thing by our customers. We aim to resolve complaints as quickly as we can, and you should hear from us within five business days (see ‘Contact Us’).

If you still feel your issue or request hasn’t been resolved to your satisfaction, then you can escalate your privacy concern (see ‘Contact details for escalating complaints’) and you have the right to make a complaint to the relevant data protection authority (for example in the place you reside or where you believe we breached your rights).

What about complaints relating to credit information?

We will let you know how we will deal with your complaint within seven days.

If we can’t fix things within 30 days, we’ll let you know why and how long we think it will take. We will also ask you for an extension of time to fix the matter. If you have any concerns, you may choose to complain to the Office of the Australian Commissioner or the French Commission Nationale de l’Informatique et des Libertés.

If your complaint relates to how we handled your access and correction requests, you may take your complaint directly to the Office of the Australian Commissioner or French Commission Nationale de l’Informatique et des Libertés. You are not required to let us try to fix it first.

Contact details for escalating complaints Need more help?

Office of the Australian Information Commissioner

- Online: www.oaic.gov.au/privacy
- Phone: 1300 363 992

- Email: **enquiries@oaic.gov.au**

Commission Nationale de l'Informatique et des Libertés (France)

- Online: https://www.cnil.fr/en/contact-cnil

- Phone: +33 (0)1.53.73.22.22

Post: 3 Place de Fontenoy, TSA 80715, 75334 Paris Cedex 07, France

Other EEA supervisory authorities

- Online: www.edpb.europa.eu, which lists all EEA supervisory authorities

- You may also complain to the supervisory authority in the EEA country where you live or work.

Contact Us

National Australia Bank Europe S.A.

Level 3, 24 rue des Capucines

75002 Paris

For more information please email us at gdpr.nabeurope@eu.nabgroup.com or visit us at www.nabeurope.com

For more information about privacy in general, you can visit the French Commission Nationale de l'Informatique et des Libertés website www.cnil.fr/en/hom

© 2022 National Australia Bank Europe S.A.