Commonwealth Bank

Candidate Privacy Statement

30 July 2026

Public

Table of contents

1. How we handle your Candidate Personal Information **3**

2. Your Privacy is important to us **3**

3. What information do we collect? **3**

4. How do we use your personal information? **5**

5. How long we keep personal information of candidates **6**

6. Who do we share your personal information with? **6**

7. Background checks **7**

8. Keeping your information safe **8**

9. Accessing, updating and correcting your personal information **8**

10. Making a privacy complaint **9**

Appendix 1: Supplementary statement concerning the General Data Protection Regulation (GDPR) 10

Appendix 2: Additional Information for Candidates in India (Digital Personal Data Protection Act, 2023) 14

1. How we handle your Candidate Personal Information

About us

The CommBank Group provides a wide range of banking and financial services. This Privacy Statement explains how the Commonwealth Bank (ABN: 48 123 123 124) and its subsidiaries handle personal information that it collects or holds for the purpose of processing job applications and managing its recruitment process.

The Commonwealth Bank of Australia and its subsidiaries (the Group) provide banking, finance, insurance, funds management, superannuation, stockbroking and other services. The Group includes CommSec, and Bankwest. All of the Group's Australian members must follow the Privacy Act and Australian Privacy Principles (APPs).

For more information about the Group, including a complete list of Group members, see CommBank's latest Annual Report, available at commbank.com.au/shareholders.

In this statement, "we", "us" or "our" refers to the Group.

2. Your Privacy is important to us

We protect your information and aim to be clear and open about what we do with it.

We understand that your privacy is important to you, and we value your trust. That's why we protect your information and aim to be clear and open about what we do with it. This statement explains how we handle your personal information.

During your relationship with us, we may tell you more about how we handle your information – for example when you complete an online application. You should always read the information provided there carefully.

Sometimes we update our Candidate Privacy Statement. You can always find the most up-to-date version on our websites.

If you wish to understand how we handle your personal information as a customer, please read our Group Privacy Statement.

3. What information do we collect?

We collect information about you, from you, when you start an application process with the Group. We may also collect information about you from other sources.

Why do we collect personal information during the recruitment process?

The personal information we collect about you will be used for the purpose of considering your potential employment with the Group in the position you may apply for or other potential positions from time to time.

What types of personal information is collected during the recruitment process?

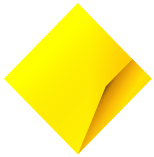
Types of personal information that we collect, use, and disclose about you during our recruitment process (offline and online) may include the following but are not limited to:

- **Contact details:** such as your name, address, phone number, and email address;
- **Employment details and qualifications:** such as information about your employment history, your qualifications such as university education, professional certification and licencing (e.g. FAR registration), and professional memberships;
- **Sensitive Personal Information**, including:
- **Health information:** such as any physical or mental condition that you choose to provide to us so that we can confirm that your ability to perform a role and to ensure that we make reasonable adjustments for your interviews and assessments where required;
- Diversity & Inclusion **information**: such as gender identity, sexual orientation, pronouns, ethnicity, ancestry, caring responsibilities, and disability information. (*Note: this information will not be used to determine your suitability for the role, and will be used for statistical reporting; and where applicable, to provide you with a personalised onboarding experience)*
- **Interview details:** such information about you that you provide during interviews or assessments (e.g. psychological and aptitude assessments) whether face-to-face, by phone, email, online, or otherwise;
- AI-generated or inferred information: such as insights inferred from work-related or recruitment-related information (for example, skills, capabilities, or development areas), generated using AI-enabled tools. These insights are used to support recruitment and talent management and are subject to human review and judgement.
- **Identity information:** such as your photo ID, passport information, birth certificates, driver licence details, date of birth, and gender;
- **Background check information:** such as criminal history details, a pre-employment medical declaration, APRA and ASIC regulatory checks, your visa status and information regarding your work eligibility, and professional references (please find more information in Chapter 7 regarding our Background check program);
- **Financial information:** such as Tax File Number (TFN), Tax Residency Status and bank account details. *(Note: In case your application is successful)*
- **Market research:** such as information you provide when you participate in a survey;
- **Location Information:** such as information about your access and use of our websites, your geo-location data through IP address or GPS;
- **Log Information:** such as information about a browser session, device and network information, statistics on page views and sessions, search queries and browsing behaviour; and
- **Cookies and Beacons:** such as log files, cookies, and similar technologies to collect and use information about the pages you view, links you click, and other actions you take when accessing our websites, services, or emails. For more information, please see our Cookie Policy.

Note that not all data types as mentioned above are requested from every candidate. Various data types may be requested depending on the stage of the recruitment process.

How do we collect personal information?

We collect personal information about you either directly from you or from third party services providers or government agencies. For instance, we work with recruitment agencies that you instructed to provide your application to us. We may also collect and use publicly available information from platforms such as LinkedIn to contact you.



4. How do we use your personal information?

We're careful about how we use your personal information.

We collect and handle personal information so we can:

- process and manage your application for employment with CBA;
- determine your eligibility for employment with CBA;
- communicate with you;
- enter into a contract with you;
- manage your onboarding with CBA;
- manage our relationship with you such as by scheduling and evaluating interviews, and to perform assessments;
- consider you for future applications (unless you request we do not consider you for future applications);
- protect our legal rights and to resolve disputes or complaints;
- comply with our legal obligations;
- manage our risks such as business continuity and security;
- understand how our websites and services are being used and to make improvements;
- diagnose website technical problems, as well as to prevent, detect, mitigate, and investigate potential security issues, as well as fraudulent or illegal activity;
- use your personal information for statistical purposes (for example, to monitor and report on diversity and equal opportunities); and/or
- use AI-enabled tools to support recruitment activities such as screening, assessment support, candidate matching, and workforce insights, with outcomes subject to appropriate human oversight and not used as the sole basis for decision-making.
- provide you with a personalised people experience (e.g. tailored onboarding content or invitations to join specific employee networks).

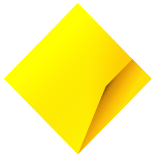
Use of AI-enabled tools

We may use AI-enabled tools to support parts of our recruitment and talent management processes, such as assisting with candidate screening, assessment support, role matching, and workforce insights. These tools are used to support decision-making and do not replace human judgement. Any outputs are subject to appropriate human review.

We may de-identify personal information we hold in connection with the recruitment and application process and use it to test and improve our AI-enabled tools. Sensitive personal information is not used for this purpose.

Talent Community

When you apply for an opportunity in the Group, you may be added to our Talent Community, where we may contact you to discuss relevant opportunities in other areas of the Group as they become available. We may use AI-enabled tools to help identify and notify you about roles that may be relevant to your experience or interests. These tools support, but do not replace, human decision-making. Through this platform we can keep you informed of other job opportunities that you might be interested in.



You will receive our quarterly updates, where we share our latest news and insights relevant to your areas of interest within the Group. You agree that you cannot unsubscribe from these Talent Community communications.

If you do not want to be part of the Talent Community, please contact your Talent Acquisition Partner.

5. How long we keep personal information of candidates

We will keep your personal information in accordance with our retention policy. The retention period may vary depending on whether your application has been successful or not. Your information may also be used for internal research and analytics.

Where your application is successful, your personal information will become part of your employee profile (employee record) with the Group. This includes all application and assessment documents (such as interview notes and test-scores), collected during the application process.

If your application for a job with us is unsuccessful, we will retain any personal information about you as long as we are required to under applicable laws or otherwise for a period of two years from the date your last application has been formally rejected.

The length of retention may also depend on whether you decide to be part of the Talent Community (see chapter 4) or if we need to respond to a question or complaint from you.

6. Who do we share your personal information with?

Why we may share your personal information:

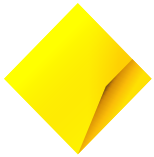
We may share your personal information with others in the following circumstances:

- where we are required or are authorised to do so by law, e.g. to assist with detecting and preventing fraud, tax evasion, money laundering, and financial crime;
- where we have a legitimate business reason for doing so, e.g. to manage risk, verify your identity or assess your suitability for roles, or to defend our legal rights and interests;
- to comply with laws and assist government or law enforcement agencies; or
- where we have your permission to do so.

With whom we may share your personal information:

We may share your information with the following entities for the purposes and circumstances described above:

- our employees, contractors, directors and officers;
- service providers who provide services to us such as recruitment agencies, IT service providers (e.g. data storage, hosting and server providers, IT security providers, vetting and background check providers, and credit reference agencies);
- law enforcement and government agencies, courts and tribunals, and any party appointed or requested by our regulators to carry out investigations;
- professional advisors, auditors, or business partners;
- fraud prevention agencies who'll also use it to detect and prevent fraud and other financial crime;
- anybody you have given us permission to share your information with; and/or



- natural or legal persons as part of a potential or actual corporate restructuring, merger, acquisition or takeover.

Third parties

We use third parties to perform certain services on our behalf. These third parties may collect, use and store personal information on our behalf, such as:

- to assess your suitability for employment;
- to manage our recruitment and application process; and,
- to conduct surveys.
- to provide AI-enabled recruitment, assessment, or workforce analytics tools that support our recruitment and talent management processes, with appropriate human oversight.

Sending information overseas

We may send your information overseas, including to:

- overseas businesses that are part of the Group;
- service providers or third parties who store data or operate outside Australia, or are involved in our recruitment process; and/or
- comply with laws, and assist government or law enforcement agencies.

This may include overseas locations where AI-enabled tools or service providers supporting our recruitment processes operate.

If we do this, we make sure there are arrangements in place to protect your information. You can find out which countries your information may be sent to at https://www.commbank.com.au/security-privacy/country-list.pdf

7. Background checks

When you apply for a role, we will conduct certain background checks. These background checks are a crucial step in the Talent Acquisition process to ensure we maintain a safe working environment dedicated to improving the financial wellbeing of our customers and communities.

The Group conducts background checks as part of complying with its legal obligations, including under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. CBA uses third party First Advantage to conduct background checks on candidates. We conduct background checks to:

- verify your identity;
- verify your right to work;
- verify your employment history, academic and professional qualifications;
- perform credit checks, conflict of interest checks, and criminal records checks in Australia and overseas; and,
- perform a Pre-Employment Medical Assessment to determine whether any reasonable adjustments are required.

During the recruitment process, we will make you aware of any relevant background checks or if the role you are applying for is subject to specific vetting requirements.

8. Keeping your information safe

Our staff are trained in how to keep your information safe and secure. We use secure systems and buildings to hold your information. We aim to only keep your information as long as we need it.

We store your hard copy and electronic records in secure buildings and systems or use trusted third parties. Here are some of the things we do to protect your information:

- Staff Training
  - › We train our staff in how to keep your information safe and secure
- Secure handling and storage
  - › When we send information overseas or use third parties that handle or store data, we put arrangements in place to protect your information
- System Security
  - › When you log into our websites or apps, we encrypt data sent from your computer to our systems so no one else can access it.
  - › We have firewalls, intrusion detection and virus scanning tools to stop viruses and unauthorised people from accessing our systems.
  - › When we send your electronic data to other organisations, we use secure networks or encryption.
  - › We use passwords and/or smartcards to stop unauthorised people getting access.
  - › Where AI-enabled tools are used, we take reasonable steps to ensure personal information is handled securely and in accordance with our existing security and risk management practices.
- Building Security
  - › We use a mix of alarms, cameras, guards and other controls in our buildings to prevent unauthorised access.

9. Accessing, updating and correcting your personal information

You can contact us and ask to view your personal information. If your information is not correct or needs updating, let us know straight away.

Can you see what information we have?

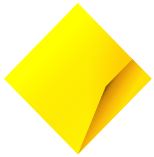
Your information will be available to you by logging in to your candidate portal. For more information, please reach out to your Talent Acquisition Partner or call HR Direct on 1800 989 696.

How long will it take?

We try to make your information available within 30 days after you ask us for it. Before we give you the information, we'll need to confirm your identity.

Can we refuse to give you access?

In some cases, we can refuse access or only give you access to certain information. For example, we might not let you see information that is commercially sensitive or would infringe the privacy of other individuals. If we do this we'll write to you explaining our decision.



Can you correct or update your information?

It's important that we have your correct details, such as your current home and email address and phone numbers. You can check and update your information by logging in to your candidate portal. If we've given the information to another party, you can ask us to let them know it's incorrect. We won't charge a fee for this. For more information on correcting and updating your personal information, please reach out to your Talent Acquisition Partner or call HR Direct on 1800 989 696.

What if we believe the information is correct?

If we don't think the information needs correcting, we'll write to let you know why. You can ask us to include a statement with the information that says you believe it's inaccurate, incomplete, irrelevant, misleading or out-of-date.

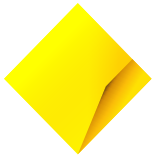
10. Making a privacy complaint

If you have a concern or complaint about how we handle personal information about you, please let us know and we'll try to fix it.

How can you make a complaint?

We try to get things right the first time – but if we don't, we'll do what we can to fix it. If you are concerned about your privacy, you can make a complaint, and we'll do our best to sort it out.

To make a complaint, please see section 9 of the CBA Group Privacy Statement.



Appendix 1: Supplementary statement concerning the General Data Protection Regulation (GDPR)

This Appendix 1 supplements the Candidate Privacy Statement and applies to the Group's processing of personal information that is governed by the GDPR.

In this Appendix 1, "personal information" means any information relating to an identified or identifiable natural person (the meaning given to the term "personal data" in the GDPR).

Personal information must be processed in a lawful, fair and transparent manner. As such, if you are located in the EU, the GDPR may require us to provide you with more information about how we collect, use, share and store your personal information as well as advising you of your rights as a "data subject".

If you are located in the EU and have an enquiry relating to your rights under the GDPR with regards to your application, please contact the HR Privacy Team.

What personal information do we collect?

Please refer to Section 3 of the Candidate Privacy Statement for details of the personal information we collect.

Special Categories of Personal Information

Note that the GDPR provides additional protection for personal information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, biometric data (for example your fingerprints), or data concerning your health, sex life or sexual orientation (known as "Special Categories of Personal Data"). We will only process these types of personal information with your consent or where otherwise lawfully permitted.

How long we keep your personal information

We will keep your personal information that we have collected through the recruitment process. We aim to keep your personal information for only as long as we need it.

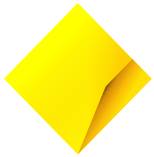
We will retain any personal information about you as long as we are required to under applicable laws or otherwise for a period of two years from the date your application has been formally rejected, but we may keep your personal information for a longer period:

- if you are part of the Talent Community;
- to fulfil legal or regulatory obligations;
- for internal research and analytics;
- to respond to a question or complaint;
- under other circumstances which require us to retain your personal information for longer, for example if you are a former employee of the Group.

How we use your personal information

We can only collect and use your personal information if we have a valid lawful reason to do so. For the Group, these reasons are:

- Contract: We need to process your personal information in order to fulfil a contract you have with us, or because you have asked us to take specific steps before entering into a contract;
- Legal obligations: we need to process your personal information for us to comply with the law (not including contractual obligations);

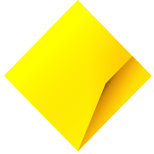


- Consent: You have given clear consent for us to process your personal information for a specific purpose;
- Legitimate interest: We need to process your personal information for our legitimate interests or legitimate interests of a third party unless there is a good reason to protect your personal information which overrides these legitimate interests.

How we use your personal information	Our reasons	Our legitimate interests
To confirm your identity	• To fulfil contracts • To meet our legal duty • We have legitimate interests	• Preventing fraud • Complying with guidance of regulators • Managing risk
To assess your job application and suitability for the role	• We have your consent • To meet our legal duty • We have legitimate interests	• Perform candidate assessments • Complying with guidance of regulators • Managing risk
To contact you	• We have your consent • To fulfil contracts • To meet our legal duty • We have legitimate interests	• To keep you updated about the recruitment process • Complying with guidance of regulators • Managing risk
To improve our service to you and your experience with us	• We have your consent • We have legitimate interests	• Ensuring high user engagement and experience • Managing risk
To comply with laws, and assist government or law enforcement agencies	• To fulfil contracts • To meet our legal duty • We have legitimate interests	• Ensuring network and information security • Complying with guidance of regulators • Managing risk
To manage our business	• We have your consent • To fulfil contracts • To meet our legal duty • We have legitimate interests	• Complying with guidance of regulators • Preventing and investigating potential criminal activity • Managing risk

Transfers of personal information to third countries

We may transfer your personal information to recipients in countries outside of the European Economic Area (so called 'third countries'), in which applicable laws may not offer the same level of data protection as the laws of your home country. When doing so, we will comply with applicable data protection requirements and, where practicable, take appropriate safeguards to ensure the security and integrity of your personal information, in particular by entering into the EU Standard Contractual Clauses. Otherwise, you acknowledge that any such transfers will take place for the implementation of pre-contractual measures taken at your request in accordance with Article 49.1(b) of the GDPR.



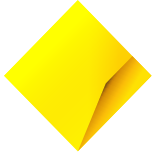
Your right as a data subject

- **The right to be informed how personal information is processed**. You have the right to be informed on how your personal information is being collected and used. If we require your consent to process your personal information you can withdraw consent at any time. If you withdraw consent, we may not be able to provide certain products or services to you. The right to withdraw only applies when the lawful basis of processing is consent.
- **The right of access to personal information.** You can access your personal information that we hold by contacting the HR Privacy team.
- **The right to rectification**. You have the right to question any personal information we have about you that is inaccurate or incomplete. If you do, we will take reasonable steps to check the accuracy and correct it.
- **The right to erasure.** You have the right to ask us to delete your personal information if there is no need for us to keep it. You can make the request verbally or in writing. There may be legal or other reasons why we need to keep your personal information and if so we will tell you what these are.
- **The right to restrict processing**. You have the right to ask us to restrict our use of your personal information in some circumstances. We may be able to restrict the use of your personal information. In this situation we would not use or share your personal information while it is restricted. This is not an absolute right and only applies in certain circumstances.
- **The right to data portability**. In some circumstances you have the right to request we provide you with a copy of the personal information you have provided to us in a format that can be easily reused.
- The right to object. In some circumstances you have the right to object to us processing your personal information.
- **Rights in relation to automated decision making and profiling.** We sometimes use systems to make automated decisions (including profiling) based on personal information we have collected from your or obtained from other sources such as credit reporting bodies. These automated decisions can affect the products or services we offer you. You can ask that we not make decisions based on automated score alone or object to an automated decision and ask that a person review.
- **The right to lodge a complaint with a supervisory authority.** If you're not satisfied with how we manage your complaint or our decision after you've been through our internal complaints process with regards to the handling of personal information, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) if you feel that your rights under the GDPR have been infringed. The individual regulator website will tell you how to report a concern.

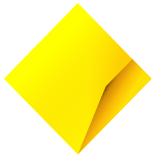
Regulator Contact Details

The UK data protection authority is:
Information Commissioner's Office
Wycliffe House, Wilmslow
Cheshire SK9 5 AF, UK
Visit: ICO.org.uk

The Netherlands Data Protection Authority is:
Autoriteit Persoonsgegevens
Prins Clauslaan 60
PO Box 93374
2509 AJ DEN HAAG / The Hague
Visit: https://autoriteitpersoonsgegevens.nl/nl



For other European jurisdictions please refer to the European Commission website for details of the relevant data protection authorities.



Appendix 2: Additional Information for Candidates in India (Digital Personal Data Protection Act, 2023)

Applicability

This Appendix supplements the Candidate Privacy Statement where the processing of your personal data is governed by the Digital Personal Data Protection Act, 2023 ("DPDPA"). Unless otherwise stated, the Candidate Privacy Statement continues to apply in full.

Collection and Processing of Your Personal Data

Please refer to Sections 3–7 of the Candidate Privacy Statement for details of the personal data we collect, the purposes for which it is processed, the parties with whom it may be shared and our background verification processes.

Consent

Where required under the DPDPA, we process your personal data with your consent or where otherwise permitted under applicable law.

By submitting your application, you acknowledge that you have read this Candidate Privacy Statement and consent to the collection, use, storage and disclosure of your personal data for the recruitment purposes described in this Statement.

Where we seek to process your personal data for additional or optional purposes (for example, to retain your details for future employment opportunities through our Talent Community), we will obtain your consent separately where required.

You may withdraw your consent at any time by contacting us using the contact details set out below. Withdrawal of consent will not affect processing undertaken before the withdrawal but may affect our ability to continue processing your application or provide recruitment-related services.

Retention of Personal Data

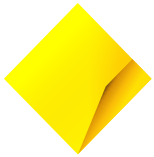
We will retain your personal data only for as long as is necessary to fulfil the recruitment purposes described in the Candidate Privacy Statement, to comply with applicable legal, regulatory or internal record-keeping requirements, or to establish, exercise or defend legal claims.

If your application is unsuccessful, we may retain your personal data for **up to two (2) years** from the date your application is formally rejected, but we may retain your personal data for a longer period if you are part of the Talent community or to fulfil any legal or regulatory obligations. Where you withdraw your consent, or where the two-year retention period expires and no other lawful basis for retention exists, your personal data will be deleted or anonymised in accordance with our retention policies and applicable law.

Your Rights under the DPDPA

Subject to applicable law, you have the following rights under the DPDPA:

- obtain information regarding the personal data being processed, the processing activities undertaken and such other information as may be available under applicable law;
- request correction or updating of inaccurate or incomplete personal data;
- request erasure of your personal data where it is no longer necessary for the purposes for which it was collected or where otherwise permitted by law;
- withdraw your consent at any time where processing is based on consent;



- nominate another individual to exercise your rights under the DPDPA in the event of your death or incapacity; and
- seek grievance redressal regarding the processing of your personal data.

We will respond to requests in accordance with applicable law.

Cross-Border Transfers

Where the DPDPA applies, transfers of personal data outside India will be undertaken in accordance with applicable law.

Grievance Redressal

If you have any questions or grievances regarding this Appendix to the Candidate Privacy Statement or wish to exercise your rights under the DPDPA, you may contact our designated Grievance Officer through workplacerelations.india@cba.com.au

If your grievance is not resolved in accordance with applicable law, you may have the right to seek remedies available under the Digital Personal Data Protection Act, 2023.

Relationship with this Statement

Except as expressly supplemented by this Appendix, the Candidate Privacy Statement continues to apply in full.

Optional Processing Activities

Where we seek your consent for optional processing activities (such as retaining your information for future employment opportunities), your decision not to provide or subsequently withdraw such consent will not affect the processing of your application for the role for which you have applied.