



Candidate Privacy Notice

Last updated April 2026

Candidate Privacy Notice

This notice (Privacy Notice) applies to personal information relating to your application for employment or engagement with HSBC Group. It explains what information we collect about you, how we'll use that information, who we'll share it with, the circumstances when we'll share it and what steps we'll take to make sure it stays private and secure. This Privacy Notice covers all aspects of your interaction with HSBC in your capacity as an applicant, including recruitment and pre-employment screening. We may update this notice at any time.

Some of the links on our websites lead to other HSBC or non-HSBC websites with their own privacy notices, which may be different to this notice. So please be aware that this Privacy Notice does not apply when you are using other websites.

Wherever we say 'you' or 'your', this means you or any authorised person who engages with us on your behalf (e.g. recruitment agencies you have authorised to liaise with us on your behalf).

When we say 'we', 'us' or 'our', we mean the HSBC Bank Bermuda Group companies and the following HSBC Bank Bermuda Group companies who will use your personal information in an applicant or candidate capacity: HSBC Bank Bermuda Limited, HSBC Institutional Trust Services (Bermuda) Limited, HSBC Securities Services (Bermuda) Limited, HSBC Global Asset Management (Bermuda) Limited and HSBC Insurance (Bermuda) Limited. Unless otherwise stated below, the primary user of your personal data for the purposes of this notice will be the HSBC Bank Bermuda Limited.

The address for the HSBC Bank Bermuda Group companies is 37 Front Street, Hamilton, Bermuda HM12. If you'd like to get in touch with us, you can find contact details set out in the '**More details about your information – How to contact us**' section below.

What information we collect

We'll only collect your information in line with relevant regulations and law. We may collect it from a range of sources, and it may relate to any of the roles you apply for, the role you currently hold or have held in the past, both within and outside of the HSBC Group. We may also collect information about you when you interact with us, e.g. call us, visit our websites or mobile channels, or use services we make available to you in your applicant capacity (e.g. online tests). Some of it will come directly from you, e.g. when you provide ID to verify your identity or right to work. It can also come from your previous employers, other HSBC companies, or other sources you've asked us to obtain information from, or you have provided us with the details for. We might also get information from publicly available sources.

The information we collect may include:

Information that you provide to us, e.g.:

- Personal details, e.g. name, previous names, gender, date and place of birth, employment history, education, racial/ethnic origin, sexual orientation, and dietary requirements;
- Contact details, e.g. address, email address, landline, and mobile numbers;
- Information concerning your identity e.g. photo ID, passport information, National Insurance number, National ID card, birth number (or equivalent) and nationality;
- Information concerning any qualifications you hold e.g. university education, professional certifications;

- Curriculum vitae or resumes you have provided including any other documents which provide details of your qualifications and work experience;
- Health data including medical condition, health and sickness records or confirmation if you are able to perform a given position (as applicable), information about any disabilities you might have;
- Market research, and information and opinions expressed when participating in applicant surveys;
- Other information about you that you give us by filling in forms or by communicating with us (e.g. interviews or assessments), whether face-to-face, by phone, email, online, or otherwise.

Information we collect or generate about you, e.g.:

- Information we use to identify and authenticate you, e.g. your signature, or additional information that we receive from external sources that we need for compliance purposes;
- Geographic information, e.g. about which HSBC offices you visit;
- Cookies and similar technologies we use to recognise you, remember your preferences and tailor the content we provide to you – our cookie policy contains more details about how we use cookies and can be found on our local internet page.;
- Investigations data, e.g. due diligence checks, fraud, sanctions and anti-money laundering checks, external intelligence reports, content and metadata related to exchanges of information between and among individuals and organisations when conducting pre-employment checks including emails, voicemail, live chat;
- Complaints information;
- Application data including information about your individual performance in any assessments or online tests that we ask you to carry out;
- Records of correspondence and other communications between us, including email, live chat, instant messages, and social media communications;
- Information that we need to support our regulatory obligations, e.g. information about transaction details, detection of any suspicious and unusual activity and information about parties connected to you or these activities (e.g., politically exposed person and sanction checks).

Information we collect from other sources, e.g.:

- Information you've asked us to collect for you, or we collect as part of our vetting process, e.g. work references from previous employers which are treated as confidential;
- Information we collect from publicly available sources such as LinkedIn and other social media.

How we'll use your information

We'll only use your information where we have your consent, or we have another lawful reason for using it. These reasons include:

- If use of the PI is necessary in context of your present, past or potential employment relationship with us;
- If we need to use the information to enter into or carry out an agreement we have with you and/or where you are a party, or to take steps at your request with a view to entering into an agreement;
- If we need to use the information to comply with a legal obligation, or pursuant to a provision of law that authorises the use of the information;

- If we are required to comply with an order made by a court, individual or body having jurisdiction over us;
- Where (except in relation to sensitive personal information) we consider that you would not reasonably be expected to request that the use of your information should either not begin or should cease and the use of your personal information does not prejudice your rights;
- Believe the use of your information as described is in the public interest e.g. for the purpose of preventing or detecting crime or for equal opportunity monitoring and/or reporting purposes;
- To protect or defend ourselves in any legal proceedings;
- Where use is necessary to respond to an emergency that threatens life, health or security of an individual or the public;
- To disclose to a public authority which is authorised or required by statutory provision to collect personal information from us;
- Where information is publicly available to use that information for a purpose that is consistent with the purpose of its public availability; and
- To contact an individual's next of kin, or in connection with disclosure to a surviving spouse or relative of a deceased individual.

The reasons we use your information include (but are not limited to):

- To match you to job vacancies using Artificial Intelligence (AI), to send you job advertisements if you've opted-in to receiving them and information on our vacancies using the methods of communication you have specified, to notify you of decisions and to schedule interviews with you.;
- To contact you about job vacancies and company matters that may be of interest to you;
- To contact you to invite you to assessment days, open days and company events that may be of interest to you;
- To carry out your instructions, e.g. send you details of online tests or assessments;
- To manage our relationship with you, including (unless you tell us otherwise) telling you about our company, opportunities, other roles, services, and events we think may be relevant for you;
- To prevent or detect crime including fraud and financial crime, e.g. financing for terrorism and human trafficking;
- For security, staff vetting and business continuity;
- For risk management; (See Appendix 1 for more information)
- To conduct applicant surveys and data analytics, to better understand our workforce and assist us with succession planning;
- To protect our legal rights and comply with our legal obligations;
- For service, system or product development and planning, insurance, audit and administrative purposes;
- For the purpose of converting a registrant to an applicant, and an applicant to an employee or contractor; and
- Assessing your suitability for a role by reviewing your background, qualifications and any other information you have provided to us.

The lawful bases for using this information are when the use of personal information is necessary in context of your present, past or potential employment relationship with us, legal obligation and/or in order to perform our contract with you.

Further details of how we'll use your information can be found in Appendix 1 below.

How we make decisions about you

We may use automated systems to help us make decisions about the outcome of your application. We may use technology that helps us identify the level of risk involved if you apply for a job or work for us, e.g. for fraud or financial crime reasons, or to identify market misconduct through analysis of irregular trades.

Tracking or recording what you say or do

We may record details of your interactions with us. We may record and keep track of conversations you have with us including phone calls, face-to-face meetings, letters, emails, live chats, video chats and any other kinds of communication. We may use these recordings to check your instructions to us, assess, analyse and improve our service, train our people, manage risk or to prevent and detect fraud and other crimes. We may also use these recordings to make decisions about the outcome of your application. We may capture additional information about these interactions, e.g. telephone numbers that you call us from and information about the devices or software that you use. We use closed circuit television (CCTV) in and around our sites and these may collect photos or videos of you or record your voice.

Vetting

Should you apply for a job with us, HSBC or a business partner (e.g. Hire Right) will request, collect and use your personal data as part of our vetting procedures which will include criminal convictions checks and credit reference checks. This will be in order to confirm your identity, employment history and relevant qualifications with respect to a role, to comply with the law and to be able to assess and manage our risk. Please note we collect personal data directly from candidates through the application and recruitment process and throughout your employment for vetting purposes. This personal data is collected by various teams within HSBC (either based in our offshore Global Service Centres or onshore Security Risk Teams and/or HR Teams). Global vendors or other carefully selected local third parties in country may also collect personal data, on our behalf, for vetting purposes.

We will typically collect, store, and use the following categories of personal information about you:

- Personal contact details such as name (all legal and alias, current and previous names), title, addresses, telephone numbers, and personal email addresses;
- Date of birth and gender;
- National insurance number or equivalent tax identification number;
- Location of employment or workplace;
- Recruitment information (including copies of right to work documentation, confidential references and other information included in a cv or cover letter or as part of the application process);
- Information concerning any qualifications you hold e.g., university education, professional certifications; and
- Employment records (including job titles, work history, working hours, training records and professional memberships).

Vetting checks that we may perform include:

- A right to work check;
- Verification of identity;
- A credit reference check;
- A conduct check, which may include a criminal check;
- A conflicts of interest check in relation to the employment of relatives, any former employment with an external auditor and any external directorships held;
- A search of internal HSBC watch lists and external watch lists or database files provided by third parties, indicating no involvement in activities such as fraud, financial crime, money laundering or breach of sanctions; and
- A media research check indicating no involvement in activities such as fraud, financial crime, money laundering, breach of sanctions, terrorism.

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note also that in connection to your application, we may use your personal information without your knowledge or consent, where this is required or permitted by law.

Enhanced Vetting

We may conduct enhanced vetting for specific high-risk roles within HSBC. We will conduct enhanced vetting during recruitment, and periodically throughout your employment, in line with HSBC's vetting policy. If your role is identified as an enhanced vetting role, you will be required to pass a number of checks to the satisfaction of HSBC before or shortly after commencing the role.

During the recruitment process, we will make you aware of any relevant specific vetting requirements for the role you are applying for.

Criminal Convictions

We may request information about criminal convictions if it is appropriate (i.e., for regulated roles) and where we are legally able to do so. We may also collect information about criminal convictions to meet our legal obligations in connection with your employment. We may collect information about criminal convictions in any country where you have resided.

We have in place an appropriate policy and safeguards when processing such data.

Credit Reference Checks

As part of your application to us, we may perform credit and identity checks on you with one or more credit reference agencies (CRAs). We may conduct credit reference checks with CRAs in any country where you have resided.

To do this, we'll supply your personal information to CRAs (see Appendix 1) and they'll give us information about you. This will include information from your credit application and about your financial situation and financial history. CRAs will supply us with public information (including the electoral register), shared credit information, financial situation, history and fraud prevention information.

We may use this information to:

- Verify the accuracy of the data you've provided to us;
- Prevent criminal activity, fraud and money laundering;
- Manage your application(s).

We'll continue to exchange information about you with CRAs while you have a relationship with us. This information may be supplied to other organisations by CRAs. Please see Appendix 1 for more details on the CRAs.

Service improvement

We'll analyse your information to identify possible service and improvements in our recruitment process. The lawful basis for processing your information for this purpose is when the use of personal information is necessary in context of your present, past or potential employment relationship with us. We do this to improve our products and services to best meet the needs of our workers.

Data analytics

We'll analyse your information to identify relevant job opportunities and to better manage our workforce. The lawful basis for processing your information for this purpose is when the use of personal information is necessary in context of your present, past or potential employment relationship with us.

Protecting our legal rights

We may need to use your information to protect our legal rights, e.g. in the case of defending or the protection of legal rights and interests (e.g. labour law disputes); court action; managing complaints or disputes; in the event of a restructuring of companies or other mergers or acquisition. This may be in connection with action taken against you or other persons. The lawful bases for using this personal information are when the use of personal information is necessary in context of your present, past or potential employment relationship with us, to protect or defend ourselves in any legal proceedings and/or to comply with a legal obligation.

Compliance with laws and regulatory compliance obligations

We'll use your information to meet our compliance obligations, to comply with laws and regulations that apply to us and to share with regulators and other authorities that HSBC Group companies are subject to. This may include using it to help detect or prevent crime (including terrorism financing, money laundering and other financial crimes). We'll only do this on the basis that the use of personal information is necessary in context of your present, past or potential employment relationship with us and/or it's needed to comply with a legal obligation.

Who we might share your information with

We may share your information with others where lawful to do so, including where we or they:

- Have a public or legal duty to do so, e.g. to assist with detecting and preventing fraud, tax evasion and financial crime;
- Need to in connection with regulatory, reporting, litigation or asserting or defending legal rights and interests;
- Need to use your personal information in context of your present, past or potential employment relationship with us; or
- Have asked you for your permission to share it, and you've agreed.

We may share your information for these purposes with others including:

- Other HSBC Group companies and any sub-contractors, agents or service providers who work for us or provide services to us or other HSBC Group companies (including their employees, sub-contractors, service providers, directors and officers);
- Your intermediaries;
- Tax authorities, trade associations, credit reference agencies;
- Any people or companies where required in connection with potential or actual corporate restructuring, merger, acquisition or takeover, including any transfer or potential transfer of any of our rights or duties under our agreement with you;
- Law enforcement, government, courts, dispute resolution bodies, our regulators, auditors and any party appointed or requested by our regulators to carry out investigations or audits of our activities;
- Other parties involved in any disputes, grievances, and investigations;
- Fraud prevention agencies who'll also use it to detect and prevent fraud and other financial crime and to verify your identity; and
- Anybody else that we've been instructed to share your information with by you.

Sharing aggregated or anonymised information

We may share aggregated or anonymised information within and outside of the HSBC Group with partners such as research groups, universities, or advertisers. You won't be able to be identified from this information, e.g. we may share information about general employment trends to assist in research.

How long we'll keep your information

We keep your information in line with our data retention policy. For example, if you are employed by us, we'll normally keep your core data for a period of twenty years from the end of our relationship with you or as per the Group or applicable local data retention schedule. This enables us to comply with legal and regulatory requirements or use it where we need to for our lawful purposes such as dealing with any disputes or concerns that may arise. If you have applied for a job with us, and are unsuccessful, we will retain any personal data collected as part of your job application in line with local regulations or otherwise for a period of six months from the date the candidate is rejected. Your candidate profile data entered in your Career Opportunity Account will be kept for a period of two years from the date your account was last active.

We may need to retain your information for a longer period where the use of the personal information is necessary in context of your present, past or potential employment relationship with us and/or we need the information to comply with regulatory or legal requirements e.g. fighting fraud and financial crime, responding to requests from regulators, etc.

If we no longer have a reason for retaining your data, we may destroy, delete or anonymise it sooner.

Transferring your information overseas

Your information may be transferred to and stored in locations outside of Bermuda, including countries that may not have the same level of protection for personal information. When we do this, we'll ensure it has an appropriate level of protection and that the transfer is lawful. We may need to transfer your information in this way if it is necessary in context of your present, past or potential employment relationship with us, to carry out our contract with you, to fulfil a legal obligation or to protect the public interest. In some countries the law might compel us to share certain information, e.g. with tax authorities. Even in these cases, we'll only share your information with people who have the right to see it.

You can obtain more details about the protection given to your information when it's transferred outside of Bermuda by contacting us using the details in the **'More details about your information – How to contact us'** section below.

Your rights

You have a number of rights in relation to the information that we hold about you. These rights include:

- The right to access information we hold about you and to obtain information about how we use it;
- In some circumstances, the right to withdraw your consent to our processing of your information, which you can do at any time. We may continue to process your information if we have a legal obligation for doing so;
- The right to request that we rectify your information if it's inaccurate or incomplete;
- In some circumstances, the right to request that we erase your information. We may continue to retain your information if we're entitled or required to retain it;
- The right to object to, and to request that we restrict, our processing of your information in some circumstances. Again, there may be situations where you object to, or ask us to restrict, our processing of your information but we're entitled to continue processing your information and/or to refuse that request.

You can exercise your rights by contacting us using the details set out in the **'More details about your information – How to contact us'** section below. You also have a right to complain about privacy related concerns to the Bermuda Privacy Commissioner's Office by visiting www.privacy.bm or can contact the Office of the Bermuda Privacy Commissioner as set out below:

Office of the Privacy Commissioner for Bermuda
4th Floor Maxwell Roberts Building
1 Church Street
Hamilton, HM11

What we need from you

You're responsible for making sure the information you give us is accurate and up to date, and we strongly encourage you to tell us if anything changes as soon as possible.

The absence or inaccuracy of any records may affect the outcome of your application, or we may be prevented from complying with our legal obligations.

How we keep your information secure

We use a range of measures to keep your information safe and secure which may include encryption and other forms of security. We require our staff and any third parties who carry out any work on our behalf to comply with appropriate compliance standards including obligations to protect any information and applying appropriate measures for the use and transfer of information.

More details about your information – How to contact us

If you'd like further information on anything we've said in this Privacy Notice you can contact using the contact details below:

You can contact our Privacy Officer (PO) by writing to:

Attention: The Privacy Officer
Middle Office
37 Front Street, Hamilton HM11

If you are employed by us you can exercise your rights, by writing to:

Attention of Rights of Individuals Fulfilment (ROIF)
Middle Office
37 Front Street, Hamilton HM11

If you have applied for a job with us, and are unsuccessful or you have not applied for a job but have entered candidate profile data in your Career Opportunity Account, you may exercise your rights by writing to:

Attention: HR Prospects Rights – Bermuda
hrprospects.rights@hsbc.com

Changes to our Privacy Notice

This Privacy Notice may be updated from time to time. This notice was last updated **April 2026**.

HSBC Bank Bermuda Limited
37 Front Street, Hamilton,
HM 11, Bermuda

April 2026

©HSBC Bank Bermuda Limited.

All rights reserved. Issued by HSBC Bank Bermuda Limited, of 37 Front Street, Hamilton Bermuda, which is licensed to conduct Banking and Investment Business by the Bermuda Monetary Authority

Appendix 1 – How we use your information

We'll use your information for the following lawful purposes which also include when the use of personal information is necessary in context of your present, past or potential employment relationship with us or to comply with a legal obligations :

1. Application administration purposes, including:

- Carrying out recruitment activities;
- Administering and maintaining personal records;
- Business continuity and emergency management purposes;
- Assessing your performance in interviews, assessments, and on-line tests;
- Evaluating your suitability for the role and making decisions on the outcome of your application;
- The pursuit of complaints;
- Equal opportunities matters including the operation of an equal opportunities policy, identifying, or keeping under review the existence or absence of the quality of opportunity, or treatment between persons of different protected characteristics, with a view to enabling such quality to be promoted, or maintained.

2. Prevent and detect crime including, e.g. fraud, terrorist financing and money laundering: this will include monitoring, mitigation, and risk management. We do this as it is necessary in context of your present, past or potential employment relationship with us, and/or legal obligation. The personal information we have collected from you will be used to prevent fraud, other unlawful or dishonest conduct, malpractice, and other improper conduct. If any of these are detected, you could be refused certain services or employment. Your personal information will also be used to verify your identity.

We may also share your information with relevant agencies, law enforcement and other third parties where the law allows us to for the purpose of preventing or detecting crime. Additionally, we and other financial institutions may take steps to help prevent financial crime and manage risk. We'll do this because we have a legal obligation to prevent or detect crime, this will include monitoring, mitigation, and risk management. We do this as it is necessary in the context of your present, past or potential employment relationship with us, legal obligation and/or in order to perform our contract with you. The personal information we have collected from you will be used to prevent fraud, other unlawful or dishonest conduct, malpractice, and other improper conduct. If any of these are detected, you could be refused certain services or employment. Your personal information will also be used to verify your identity. We may be required to use your information to do this, even if you've asked us to stop using your information. That could include (among other things):

- Passing information to relevant agencies if we think you've given us false or inaccurate information, or we suspect criminal activity;
- Combining the information, we have about you with information from other HSBC Group companies to help us better understand any potential risk.

3. **Risk management:** we'll use your information to measure, detect and prevent the likelihood of financial, reputational, legal, compliance or customer risk. This includes credit risk, traded risk, operational risk and insurance risk (e.g. for underwriting or claims management purposes).
4. **Online assessments:** we'll use your information to allow us to provide you with access to any online platforms in order for you to carry out any relevant online tests. The platform may allow you to directly or indirectly communicate with us.
5. **Credit reference checks:** we may perform credit and identity checks on you with one or more credit reference agencies (CRAs). We may conduct credit reference checks with CRAs in any country where you have resided.

To do this, we'll supply your personal information to CRAs and they'll give us information about you. This may include information from your credit application (if applicable) and about your financial situation and financial history. CRAs will supply us with public information (including the electoral register), shared credit information, financial situation, history, and fraud prevention information.

We may use this information to:

- Prevent criminal activity, fraud, and money laundering; and
- Manage your employment.

We'll continue to exchange information about you with CRAs while you have a relationship with us. This information may be supplied to other organisations by CRAs.