

Data Privacy Notice

HR Data Privacy Notice

Before we begin

This notice (Privacy Notice) applies to personal information relating to your employment or engagement (prospective, current or former) with HSBC Group held by members of the HSBC Group as data controllers, as described below. 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 should also be read alongside your employment or engagement terms, as these might include sections relating to the use and disclosure of information. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

This Privacy Notice covers all aspects of your interaction with HSBC in a worker capacity, including recruitment, onboarding, performance management, learning, employee relations (which would include for example if you were to raise a formal grievance or be involved in a disciplinary process), payroll, workforce administration. It also covers any benefits and or rewards we provide to you as part of your employment (e.g., share plans) which you hold, even after your employment or engagement with us ends. Sometimes we may need to provide you with separate or further information about specific services like global mobility or learning. This information will also apply.

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. You'll need to make sure you're happy with their privacy notices when using those other sites.

Wherever we've said 'you' or 'your', this means you or any authorised person who engages with us on your behalf (e.g. trustees or executors, attorneys under a Power of Attorney, and or recruitment agencies you have authorised to liaise with us on your behalf).

When we say 'we', we mean HSBC Group companies (as set out in Appendix 1) which act as a data controller in respect of your personal data in your worker capacity. Unless otherwise stated below, the data controller for the purposes of this notice will be the HSBC Group company that is your employer.

The HSBC Group companies outlined in Appendix 2 will act as a data controller where you hold a product or service with them. There may also be products or services you receive as part of your employment or engagement that are provided by or involve other HSBC entities and or external third parties. In these cases, those other HSBC entities and or external third party may be the data controller for these products or services.

If you'd like to get in touch with us, you can also find contact details set out in the 'More details about your information' 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, 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 worker capacity.

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. We might also get some of it 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;
- contact details, e.g. address, email address, landline and mobile numbers;
- next of kin and emergency contact details;
- information concerning your identity e.g. photo ID, passport information, National Insurance number or equivalent tax identification number, National ID card, birth number (or equivalent) and nationality;
- information concerning any qualifications you hold e.g., university education, professional certifications;
- health data including medical condition, medical related absence records, health and sickness records or confirmation if you are able to perform a given position (as applicable), information about any disabilities you might have;
- information necessary to pay you e.g., bank account details, or to provide you with benefits, e.g., dependants and beneficiaries, driving license details' for car schemes we may operate etc.;
- market research, information and opinions expressed when participating in worker surveys;
- other information about you that you give us by filling in forms or by communicating with us, 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, additional information that we receive from external sources that we need for compliance purposes;
- geographic information, e.g. about which HSBC offices you access;
- benefits and rewards information, e.g. details of the services and products you subscribed to;
- 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 your local intranet page;
- investigations data, e.g. due diligence checks, fraud, sanctions and anti-money laundering checks, external intelligence reports, content and metadata related to relevant exchanges of information between and among individuals, organisations, including emails, voicemail, live chat, and any opinion you express in relation to any issues that are the subject of an investigation;
- complaints, disciplinary and grievance information;
- succession planning and workforce management data including information about your individual performance in roles you held with us;
- 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 and risk management 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 as set out below, e.g. work references from previous employers and information about your previous roles with us.

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 where we:

- need to pursue our legitimate interests (e.g., to offer participation in a share plan or benefit scheme with us);
- need to process the information to carry out an agreement we have with you;



- need to process the information to comply with a legal obligation;
- 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).

The reasons we use your information include:

- to administer your worker relationship with us;
- to carry out your instructions, e.g. with regards to any benefits selections you make;
- to manage our relationship with you, including (unless you tell us otherwise) telling you about roles, products and services we think may be relevant for you;
- to provide products and or services to you as part of your employment (e.g., employee benefits such as life insurance or accidental insurance etc.), as applicable;
- to administer a share plan or deferred reward you may hold with us;
- to prevent or detect crime including fraud and financial crime, e.g. financing for terrorism and human trafficking or market abuse;
- to contact you or your emergency contacts in the event of an emergency;
- for security, staff vetting or business continuity;
- for risk management;
- to conduct worker 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.

Further details of how we'll use your information can be found in Appendix 3 below.

How we make decisions about you

We may use automated systems to help us make decisions, e.g. to assess your skillset and suitability for a role and or through the use of online assessments, as part of our recruitment processes. We may use technology that helps us identify the level of risk involved in your work for us, e.g. for fraud or financial crime reasons, or to identify market misconduct through analysis of irregular trades.

You may have a right to certain information about how we make these decisions. You may also have a right to request human intervention and to challenge the decision. More details can be found in the 'Your rights' section below.

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 on the future of your employment. 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

We will request, collect and process your personal data as part of our vetting procedures. 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 for our legitimate interests to be able to assess and manage our risk.



We collect personal data for vetting through the application and recruitment process directly from candidates by 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 for vetting purposes for us.

The personal information we will typically collect, store, and use for vetting purposes will include the following categories of personal information:

- personal contact details such as name (all legal and alias, current and previous names), title, addresses, telephone numbers, and personal email addresses;
- information on family members and or dependents;
- 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, 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;
- 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;
- tax compliance or solvency related information to the extend required by law;
- a conduct check, which may include a criminal check (we will only conduct criminal checks where legally permitted or required);
- 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.

In some markets, we may perform 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 we may process 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 posts within HSBC. We will conduct enhanced vetting during recruitment, and periodically throughout your employment, in line with the vetting policy (available on the HSBC intranet [here](#)). 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. A list of roles subject



to enhanced vetting is provided [here](#) and a list of checks that may be completed can be found [here](#). During the recruitment process, we will make applicants aware of any specific vetting requirements of the post in question.

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 for a period of six months or more within the last five years, where we are legally able to do so.

We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data.

Credit Reference Checks

As part of your employment with us, we may perform credit and identity checks on you with one or more credit reference agencies (CRAs). We will conduct credit reference checks with CRAs in any country where you have resided for a period of 6 months or more within the last five years.

To do this, we'll supply your personal information to CRAs 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 both public (including the electoral register) and shared credit information, financial situation, history and fraud prevention information.

We may use this information to:

- prevent criminal activity, fraud and money laundering;
- 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.

For workers in the UK, please see Appendix 3 for more details on the CRAs.

Compliance with laws and regulatory compliance obligations

We'll use your information to meet our compliance obligations, to comply with other laws and regulations 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 it's needed to comply with a legal obligation or it's in our legitimate interests or that of others.

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, tax or withholding reporting, litigation or asserting or defending legal rights and interests;
- have a legitimate business reason for doing so, e.g. to manage risk, verify your identity, enable another company to provide you with services you've requested, or assess your suitability for products and services;
- have asked you for your permission to share it, and you've agreed;
- need to in order to provide you with products or services you've requested, e.g. sharing your details with a healthcare insurance company or our chosen share plan administrator.

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 beneficiaries or 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;
- anybody else that we've been instructed to share your information with by you;
- third party benefits providers.

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 and or universities. 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 we'll normally keep your core employment data for a period of seven 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 legitimate purposes such as dealing with any disputes or concerns that may arise. If you have applied for a job with HSBC, and are unsuccessful, we will retain any personal data collected in line with local regulations or otherwise for a period of two years from the date you are formally rejected.

We may need to retain your information for a longer period where we need the information to comply with regulatory or legal requirements or where we may need it for our legitimate purposes, e.g. to help us respond to queries or complaints, fighting fraud and financial crime, responding to requests from regulators, etc.

If we don't need to retain information for this period of time, we may destroy, delete or anonymise it more promptly.

Transferring your information overseas

Your information may be transferred to and stored in locations outside the European Economic Area (EEA), 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 to carry out our contract with you, to fulfil a legal obligation, to protect the public interest and / or for our legitimate interests. 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 of the protection given to your information when it's transferred outside the EEA by contacting us using the details in the 'More details about your information' 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 process it;
- 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 another legitimate reason or legal obligation for doing so;
- in some circumstances, the right to receive certain information you have provided to us in an electronic format and / or request that we transmit it to a third party;
- 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' section below. You also have a right to complain to the data protection regulator in the country where you live or work.

What we need from you

You're responsible for making sure the information you give us is accurate and up to date, and you must tell us if anything changes as soon as possible. If you provide information for another person (e.g., where you provide information or details of dependants and or beneficiaries for healthcare or life insurance coverage), you'll need to direct them to this notice and make sure they agree to us using their information as described in it.

The absence or inaccuracy of any records may affect the provision of certain benefits, the performance of any contracts that we have entered into with you, 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

If you'd like further information on anything we've said in this Privacy Notice contact us via [HR Direct](#), your usual HR representative or your line manager.

Appendix 1 – Legal Entities

Country	Legal Entity
Belgium	HBEU Belgium Branch
Czech Republic	HBEU Czech Republic Branch
France	HSBC Assurances Vie (France)
France	HBEU France Branch
France	HSBC France
France	HSBC Global Asset Management (France)
Germany	HSBC Global Asset Management (Deutschland) GmbH
Germany	HSBC Trinkaus & Burkhardt AG
Germany	HSBC Trinkaus Real Estate GmbH
Germany	HSBC Transaction Services GmbH
Germany	INKA Internationale Kapitalanlagegesellschaft mbH
Greece	HSBC France, Greece Branch
Ireland	HBEU Ireland Branch
Ireland	HSBC Institutional Trust Services (Ireland) DAC
Ireland	HSBC Securities Services (Ireland) DAC
Italy	HBEU Italy Branch
Luxembourg	HBEU Luxembourg Branch
Luxembourg	HSBC Investment Funds (Luxembourg) SA
Luxembourg	HSBC Private Bank (Luxembourg) S.A.
Malta	HSBC Global Services (UK) Ltd – Malta Branch
Malta	HSBC Bank Malta p.l.c.
Netherlands	HBEU Netherlands Branch
Poland	HSBC Bank Polska S.A.
Poland	HSBC Service Delivery (Polska)
Spain	HBEU Spain Branch
Switzerland	HSBC GLOBAL ASSET MANAGEMENT (Switzerland) AG
Switzerland	HBEU Switzerland Branch
Switzerland	HSBC Trust Company AG
Switzerland	HSBC Private Bank (Suisse) SA
Switzerland	HSBC PB Services (Suisse) SA
Switzerland	HSBC Private Banking Holdings (Suisse) SA
UK	HSBC Global Asset Management (UK) Limited
UK	HSBC Global Asset Management Limited
UK	HSBC Global Asset Management (International) Limited
UK	HSBC Alternative Investments Limited
UK	HSBC Asia Holdings B.V.
UK	HSBC Bank plc UK Ops
UK	HSBC Bank International Limited
UK	HSBC UK Bank plc
UK	HSBC Group Management Services Limited
UK	HSBC Global Services (UK) Limited
UK	HSBC Trustee (Guernsey) Limited
UK	HSBC Management (Guernsey) Limited

UK	HSBC Securities Services (Guernsey) Limited
UK	HSBC Trustee (C.I.) Limited
UK	Marks and Spencer Financial Services plc
UK	HSBC Private Bank (UK) Limited

Appendix 2 – List of HSBC Legal Entities providing a product or service

Country	Product or service	Legal Entity
Various (benefit provided from the UK)	Share Plan; Deferred Rewards	HSBC Holdings Plc
UK	Life insurance; critical illness; group income protection insurance	HSBC Life (UK) Limited

Appendix 3 – How we process your information

We'll use your information for purposes including:

1. Worker administration purposes, including:

- Carrying out recruitment activities;
- Administering and maintaining personal records;
- Payroll functions and paying and reviewing remuneration, including any deferred rewards;
- Providing, administering and reviewing benefits, for example, pension and retirement savings, share plan, private health insurance, life insurance, accidental insurance, permanent health insurance, and provision of occupational health services;
- Business continuity and emergency management purposes;
- Maintaining medical records, including information about your physical and mental health or condition in connection with occupational health matters, or confirmation of your medical check to confirm your ability to work (as appropriate);
- Maintaining holiday records, absence returns and sick leave/pay information;
- Taking decisions about an employee's fitness for work;
- Carrying out performance reviews and appraisals;
- The pursuit of disciplinary and grievance matters;
- Compiling lists of experience for clients, pitches, training and recruitment;
- Providing information to future employers, regulators and, if necessary, governmental and quasi-governmental bodies for social security and other purposes;
- Maintaining maternity, paternity and adoption leave/pay information;
- Maintaining other absence records, for example, on parental leave or time off to care for dependants;
- 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.

The lawful reasons for processing these are legitimate interest, legal obligation and in order to perform our contract with you.

- ### 2. To prevent and detect crime including, e.g. fraud, terrorist financing and money laundering:
- this will include monitoring, mitigation and risk management. We do this to comply with our legal obligations and because it's in our legitimate interest. We may 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 (for e.g., we may upload staff information into third party fraud prevention databases where we have evidence of an act of fraud). 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 legitimate interest, a legal obligation to prevent or detect crime or it's in the public interest. 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 companies to help us better understand any potential risk.

- 3. Internal IT systems:** we'll use your information to allow us to provide you with access to HSBC internal IT systems, online platforms and mobile apps. The platform may allow you to directly or indirectly communicate with us through mobile apps, or applying for products and services online. The lawful basis for using your information for this purpose is to perform our contract with you or that processing for this purpose is in our legitimate interest;
- 4. Product and service improvement:** we'll analyse your information to identify possible service and product improvements. The lawful basis for processing your information for this purpose is our legitimate interest. We do this to improve our products and services to best meet the need of our workers;
- 5. Data analytics:** we'll analyse your information to identify relevant job opportunities and to better manage our workforce. The lawful basis for using your information in this way is our legitimate interest;
- 6. 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. We'd do this on the basis that it's in our legitimate interest;
- 7. Credit Reference Checks:** for workers in the UK, the identities of the CRAs, their role also as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and your data protection rights with the CRAs are explained in more detail at:
 - Call Credit – www.callcredit.co.uk/crain
 - Equifax – www.equifax.co.uk/crain
 - Experian – www.experian.co.uk/crain