

Applicant Privacy Notice

Before we begin

This Privacy Notice covers all aspects of your interaction with us in your capacity as an applicant, including recruitment and pre-employment screening for the relevant job position.

Some of the links on our websites lead to other HSBC companies or non-HSBC websites with their own applicant privacy notices, which may be different to this notice. You will need to make sure you are comfortable with their privacy notices when using those other sites.

Wherever we have said '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' or 'us', we mean HSBC Continental Europe(France) and its European Branches.

HSBC Continental Europe (France) and its European branches, as independent Data Controllers, have appointed a Data Protection Officer that you may contact for matters related to processing your personal information via e-mail at: - dataprotection@hsbc.fr, or by post at:

HSBC Continental Europe, Data Protection Officer
38 Avenue Kléber
75116 Paris

If you would like to get in touch with us, you may also find our contact details in the 'More details about your information' section below.

What information we collect

We will only collect your data in line with relevant regulations and law. The collected data 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 HSBC Continental Europe.

Some of the information will come directly from you, e.g. when you send your application. However, we may also collect information about you when you visit our websites or mobile channels, conduct interviews either online or onsite or use services we make available to you in your applicant capacity (e.g. online tests online tests)

The data we collect may include:

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

- personal details, e.g. name, previous names, gender, date of birth, employment history;
- contact details, e.g. address, email address, landline and mobile numbers;
- information concerning your identity e.g., National ID card (as appropriate) and nationality;
- information concerning any qualifications you hold e.g., university education, professional certifications;
- company doctor confirmation/report 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;
- cookies and similar technologies we use to recognise you, remember your preferences and tailor the content we provide to you – HSBC Continental Europe cookie policies (relevant to each HBCE jurisdiction) contain more details about how we use cookies and can be found in the Appendix 2 below
- investigations information, e.g. due diligence checks,
- complaints information;
- application data including data about your individual performance in assessments or online tests;
- records of correspondence and other communications between us, including email, live chat, instant messages
- data that we need to support our regulatory obligations, 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).

How we'll use your information

We will 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 assess your suitability for the role you are applying for);
- need to process the information to comply with a legal obligation;

The reasons we use your information include:

- to administer your applicant relationship with us e.g. schedule interviews, communicate decisions etc.;
- 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 other roles 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, vetting and business continuity
- for risk management;
- to conduct applicant surveys and data analytics, to assist us with improvements on our recruitment processes;
- to protect our legal rights and comply with our legal obligations;
- for service, system or product development and planning, audit and administrative purposes.

Further details of how we will 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, e.g. when you apply for a new role, or to carry out fraud and money laundering checks. 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 -subject to your consent- 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, and manage risk. We may also use these recordings to make decisions on 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) for security reasons in and around our sites and these may collect videos of you.

Vetting

We will request, collect and process your personal information 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 information 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 information for vetting purposes for us.

Our Teams and vendors may collect your data from the following external sources:

Local Departments of Justice – for the purposes of our criminal records checks (where applicable)

Former Employers (with your approval) – for the purposes of our professional reference checks

Universities- for the purposes of our academic reference checks (where applicable)

Search Engines – in particular Google – for the purposes of our media checks (where applicable)

Social Media – in particular LinkedIn – for the purposes of our media checks (where applicable)

International Screening Databases – more specifically the Refinitiv Worldcheck Database- which enable us to screen candidate names against Sanctions/ Embargo Lists, Money Laundering Lists, Politically Exposed Person Lists, Fraud Lists, Law Enforcement Lists and Regulatory Enforcement Lists

Our Teams and vendors will typically collect, store, and use the following categories of personal data:

- 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 (if relevant);
- location of employment or workplace;
- recruitment data (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 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 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 only if it is required for regulated roles)

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;
- have a legitimate business reason for doing so, e.g. to manage risk, verify your identity or assess your suitability for roles; and
- have asked you for your permission to share it, and you have agreed.

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

- any sub-contractors, agents or service providers who work for us or provide services to us;
- 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 engagement 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 will also use to verify your identity;
- anybody else that we have been instructed to share your information with by you.

Sharing aggregated or anonymised data

We may share aggregated or anonymised information within and outside of the HSBC Continental Europe with partners such as research groups, universities or advertisers. You will not be able to be identified from this information, e.g. we may share information about general recruitment trends to assist in research.

How long we will keep your information

We keep your information in line with our information retention policy, meaning that we limit the retention time of your personal data to a strict minimum. If the application is successful, the information you shared with us during the application procedure will be added to your personal file and will be kept in line with the information retention policy and the Employee Data Privacy Notice a copy of which you shall receive upon your engagement. If you have applied for a job with HSBC, and are unsuccessful, we will retain any personal information collected in line with local regulations or otherwise for a period of five years from the date the recruitment application process has been closed.

If you are required to complete an on-line assessment as part of your application, your test results may be valid for future job applications and we will keep them, unless you instruct us otherwise, for a period of twelve months. After twelve months your test results will be deleted and therefore if you apply to either the same role or a different role with us in the future then you may be required to complete a new on-line assessment.

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 do not need to retain information for a longer period of time, we may destroy, delete or anonymise it more promptly.

Transferring your data 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 will ensure that the European Commission's Standard Data Transfer Clauses (SCC's) are included within the relevant contracts. We may need to transfer your information in this way to carry out the recruitment process and / or to fulfil a legal obligation, to protect the public interest and / or for our legitimate interests. Even in these cases, we will 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 is 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 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 is 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 are 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 Authority or by visiting their website (see Appendix 2 below)

What we need from you

You are 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.

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 data 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 data.

More details about your information

If you would like further information on anything we've said in this applicant Privacy Notice contact HSBC Continental Europe's Data Protection Officer at: dataprotection@hsbc.fr.

Appendix 1 – How we process your information

We'll use your information for purposes including:

1. Application administration purposes, including:

- carrying out recruitment activities;
- administering and maintaining personal records within the capacity of application and recruitment process;
- 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.

The lawful reasons for processing these are in order to take steps at the request of the data subject prior to entering into a contract, legitimate interest, legal obligation (art. 6 point 1 letter b, c and f of GDPR).

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 because it is 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. Additionally, we and other financial institutions may take steps to help prevent financial crime and manage risk. We will do this because we have a legitimate interest, a legal obligation to prevent or detect crime or it is in the public interest (art. 6 point 1 letter f, c and e of GDPR). We may be required to use your information to do this, even if you have asked us to stop using your information. That could include (among other things):

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

3. Risk management: we will 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). We will do this because we have a legitimate interest in ensuring that we carry out a proper risk assessment prior to making offers of employment (art. 6 point 1 letter f of the GDPR);

4. Online assessments: we will 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. The lawful basis for using your data for this purpose is in our legitimate interest (art. 6 point 1 letter f of the GDPR);

5. Service improvement: we will analyse your information to identify possible service and improvements in our recruitment process. The lawful basis for processing your data for this purpose is our legitimate interest (art. 6 point 1 letter f of the GDPR). We do this to improve our products and services to best meet the need of our future and current workers;

6. Data analytics: we will analyse your information to identify relevant job opportunities and to better manage our recruitment processes. The lawful basis for using your data in this way is our legitimate interest (art. 6 point 1 letter f of the GDPR);

7. **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 would do this on the basis that it is in our legitimate interest (art. 6 point 1 letter f of the GDPR).

Appendix 2 – HSBC Continental Europe - Useful Links and Contact Points

This applicant notice applies to the processing of personal data relating to your application for employment with HSBC Continental Europe (France) or any of its European branches. In the recruitment context, each HSBC Continental Europe branch serves as an independent data controller within the meaning of the General Data Protection Regulation. This notice covers applications to:

1. **HSBC Continental Europe France – established at 38, avenue Kléber, 75116, Paris**

Cookie Notice Available at: <https://www.hsbc.fr/cookies/>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

2. **HSBC Continental Europe Belgium- established at Square de Meeûs 23, 1000 Brussels**

Cookie Notice Available at: <https://www.hsbc.be/en-gb/cookie-policy-page>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

3. **HSBC Continental Europe Netherlands- established at De Entree 236, 1101 EE Amsterdam**

Cookie Notice Available at: <https://www.hsbc.nl/en-gb/cookie-policy-page>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

4. **HSBC Continental Europe Luxembourg- established at 16 Boulevard d'Avranches, 1160 Luxembourg**

Cookie Notice Available at: <https://www.hsbc.lu/en-gb/cookie-policy>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

5. **HSBC Continental Europe Spain-** established at Plaza Pablo Ruiz Picasso, 1, 28020 Madrid,

Cookie Notice Available at: <https://www.hsbc.es/es-es/cookie-notice>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

6. **HBCE Continental Europe Italy-** established at: Via Mike Bongiorno, 13, 20124 Milano MI

Cookie Notice Available at: <https://www.hsbc.it/en-gb/cookie-policy>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

7. **HSBC Continental Europe Greece-** established at: 109-111 Messoghion Ave., Athens.

Cookie Notice Available at: <https://www.hsbc.gr/cookie-notice/>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

8. **HSBC Continental Europe Czech Republic,** established at Na Florenci 2116/15, 110 Praha 1, Czech Republic.

Cookie Notice Available at: <https://www.hsbc.cz/en-gb/cookie-policy-page>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

9. **HSBC Continental Europe Sweden and Nordics –** established at : Birger Jarlsgatan 4, 2nd floor, SE 114 34, Stockholm

Cookie Notice Available at: <https://www.business.hsbc.se/en-gb/se/generic/cookie-policy>

DPO Contact: Alexandre Moizan – DPO HSBC Continental Europe - dataprotection@hsbc.fr

