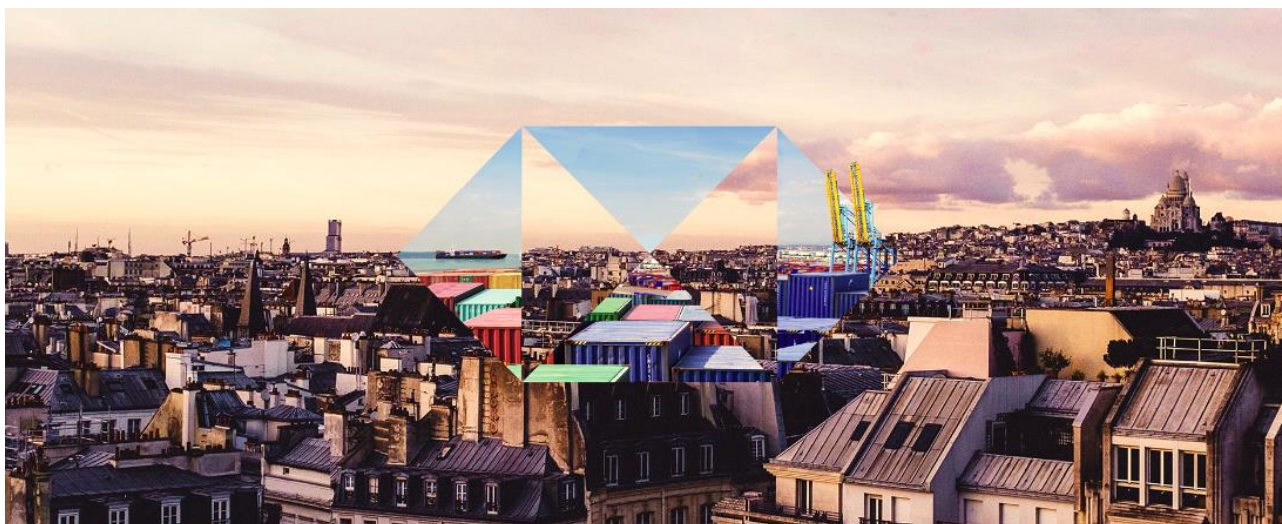


## Personal Data Protection Policy



### How are your personal data collected, stored and processed?

#### Before you start

This Policy applies to all personal data processed by HSBC Group entities in France acting as data controllers. It explains how we use this data, with whom we are likely to share it, and what steps we take to ensure their privacy and security. The policy applies even if the agreement relating to banking or other products or services ends.

This Policy covers all the personal data processing of which the controller is HSBC Continental Europe (including HSBC Private Banking), HSBC Assurance Vie (France) or HSBC REIM. If you are in contact with other HSBC entities, specific information will be provided to you if necessary.

Some of the links on our websites may redirect you to non-HSBC websites. They have their own policies or privacy or data protection charters that may differ from ours: it is your responsibility to read them.

When we use the terms “you” or “your”, it means you, or any authorised individual, including holders of joint accounts, any person who may carry out your banking, insurance or financial instrument transactions and SCPI with our services and any other person within your company (including your agents and signing officers, spouses, contacts, subscribers or holders of life insurance policies or endowment bonds or their representatives, etc.).

Similarly, when we use the terms “HSBC”, “we” or “our”, this includes all HSBC entities in France and other HSBC Group companies. HSBC Group refers to all companies owned and/or controlled directly or indirectly by HSBC Holdings Plc as control is understood within the meaning of Article L.233-3 of the French commercial code.

#### **What data do we collect?**

The data we collect or hold about you may come from a variety of sources. Some data have been collected directly from you, while other data may have been collected in accordance with applicable regulations in the past or by other companies of the HSBC Group. We may also collect information about you when you interact with us, for example when you visit our websites or when you use our mobile applications, when you call us or visit one of our branches.

Some may even come from publicly available sources (for example, creditors' registers, the press and Internet sites) or from external companies (credit control agencies, for example). We may also collect data by combining datasets (for example, location data if you have a mobile application provided that geolocation is enabled).

- The data you provide us may, for example, relate to:
  - information about your identity such your name, gender, date and place of birth, the information on your credentials;
  - your contact information such as your mailing address, email address, and telephone numbers;
  - information you provide to us by completing forms or contacting us by phone, in person, by email or by any other means of online communication or by responding to questionnaires or satisfaction surveys.
  
- The data we collect or generate may include:
  - information about our business relationship, your transactions and instructions (including information about your accounts or assets held with other financial institutions), the channels of communication you use with us, your ability to repay your loans, your solvency, your transaction histories, the transactions generated on your accounts, your claims;
  - the information we use to identify and authenticate you such as your signature sample, your biometric information such as your voice and any other information we may receive from external sources to ensure our identity;
  - geographic location data (about the branches you visit or ATMs you use);
  - any information contained in the client documentation (investor profile, account statements, etc.) or forms that you could complete as a prospect;
  - any information of a commercial nature, such as the details of the products or services you benefit from;
  - data collected through “cookies”. We use “cookies” and similar technologies on our websites and in email messages to recognise you, remember your preferences and present you with content that may be of interest to you.  
Consult [our cookie policy](#) for more details on how we use cookies;
  - information about your risk rating, such as your credit risk rating or transactional behaviour;
  - data related to our internal investigations, in particular the controls relating to the pre-contact checks or throughout our commercial relationship, the controls relating to the application of the rules on sanctions, the freezing of assets, the fight against money laundering and the financing of terrorism and all information related to controls on our means of communication;
  - records of all correspondence and communications between us, including phone calls, email messages, instant messaging, social media communications or any other type of communications and exchanges;
  - any information we need to comply with our legal and regulatory obligations, including your financial transaction data, the information necessary to detect any suspicious or abnormal activity concerning you or the persons with whom you are in contact.
  
- The data we obtain from other sources may include:
  - communication information (for example, information contained in email messages, third party information, chat information, instant messages, media information, disputes and parties involved and transcriptions or minutes); and
  - information that you have asked us to collect for you (information about your accounts or assets held with other financial institutions).

## **How do we use your data?**

We will only use your personal data if you have consented to it or if it is based on one of the legal grounds laid down by law:

- The protection of our legitimate interests;
- The performance of a contract or commitment for which you are and/or we are engaged;
- Compliance with a legal or regulatory obligation;
- The preservation of the public interest, such as the prevention or detection of fraud or financial crimes.

We collect and process information about you for a variety of reasons, including to:

- provide you with products and services;
- carry out your instructions and our commitments to you (including insurance policies);
- manage our commercial relationship with you – including (unless you refuse) offering you our products, contracts and services or carrying out market research;
- understand the functioning of your account and the use of your services;
- facilitate and provide assistance with banking operations (notably computer support);
- collect information from the analysis of your data;
- improve the quality of our products, contracts and services and ensure the effectiveness of our marketing campaigns;
- keep a record of our exchanges with you (by phone, in person, by email or any other type of communication);
- prevent or detect any risk of fraud or financial crime;
- ensure the continuity of the activity of our services;
- correspond with our lawyers, counsel or other stakeholders (subcontractors, suppliers, carriers, partners or other interested third parties);
- manage our internal operational needs in terms of credit and risk management, development and planning of computer systems or products, insurance policies, SCPI shares or auditing;
- defend our rights and respect our legal, regulatory or tax obligations.

Sometimes, you may have expressed your willingness not to see your data used but we still have to use it for different reasons. In such a case, we will continue to use them if (i) the law requires us to do so, (ii) if we are required to perform a contractual obligation, (iii) if it is in the public interest to do so or (iv) if we have a legitimate interest in doing so.

## **[Appendix 1: list of purposes]**

### **Automated decisions**

We are likely to use automated systems to assist decision making, for example when you want to subscribe to a product or a service, when you are seeking a loan or during controls aiming to prevent the risk of fraud, money laundering or financing of terrorism. We may use such processes to help us determine whether the activity of a client or account involves a risk (credit, fraud or financial crime). For example, we can use this process to determine if your credit card is used fraudulently.

You are entitled to specific information about how a decision is made, to request human intervention and to challenge any decision made on these grounds. Please see the “Your Rights” section below for more information.

### **Follow-up and recording of our exchanges**

We may record and retain conversations that you have with us – including phone calls, face-to-face meetings, letters, email messages, live chats, video chats and any other type of messaging – to check your instructions. We may also evaluate, analyse and improve our services, train our employees, manage risks or prevent and detect fraud and other financial crimes from these data.

We use a video surveillance system in and around our branches and offices for security purposes, so we may collect images, photos, or videos from you, or record your voice through this process.

### **Compliance with our legal and regulatory obligations**

We use your personal data to comply with our obligations, comply with any applicable law or regulation and, where appropriate, share your data with a regulator or a competent authority in strict compliance with applicable law. The purpose of this use is to detect or prevent any risk of financial crime/offence (including terrorist financing, money laundering) and is based on a legal obligation or on our legitimate interest.

### **Marketing and market research:**

Your personal data may be processed to promote its products and services. If you agree, we may send you commercial messages (email, SMS, phone, secure email from your Online Banking) containing information about our products and services or those of third parties.

You may withdraw your consent to the use of your data for commercial purposes at any time: taking into account your request and updating our systems may take a few days during which you are likely to receive commercial solicitation requests concerning marketing campaigns already launched. To ask us to stop sending you marketing messages or to use your data for marketing purposes, including to adapt our content or advertising to your profile when you use one of our websites, please refer to the section “More details about your data”. You may also withdraw your consent to these marketing activities or operations when you use our websites or when you interact with your client adviser.

Branches in charge of carrying out market research may contact you (by post, telephone, email or any other means of communication) to invite you to take part in a study. You may withdraw your consent to use your data for market research purposes at any time. If this is the case, we will stop using your data for this purpose.

### **With whom are we likely to share your data?**

We may share your personal data for the following reasons:

- to provide you with products or services that you have requested, such as opening an account, responding to a subscription request or performing your instructions;
- to comply with a legal or regulatory obligation (e.g. to help detect fraud or tax evasion, to prevent financial crimes);
- to respond to a request for regulatory reports, to manage litigation or to act in defence of our rights;
- to act on the basis of a legitimate interest, for example to manage an operational risk or evaluate the relevance or effectiveness of our commercial campaigns of our products or services;
- to act in accordance with your consent, previously collected.

We may transfer and disclose your data to:

- other companies of the HSBC Group;
- subcontractors, authorised agents or service providers who work for us or other HSBC Group companies (including their employees, directors and officers);
- co-holders of accounts, persons who carry out your banking transactions for you, your beneficiaries, intermediary banks, correspondents and depositories, clearing houses, any market participant or counterparty, stock exchanges or any company in which you hold financial instruments through us (for example, stocks or bonds);
- other financial institutions, tax authorities, professional associations, credit control agencies and debt collection agencies;
- fund managers who provide you with asset management services and all distributor intermediaries and brokers who put you in touch with us or deal with us on your behalf;
- any person, company or other person who has an interest in or assumes a risk with respect to or in connection with the products or services we provide to you;
- any company (new or potential) of the HSBC Group (for example, if we restructure or acquire other companies or merge with other companies) or any company that acquires all or part of an HSBC group company;
- auditors, regulators, the TRACFIN unit, Banque de France (in the event of registration in the Central Cheques register – FCC or the National Database on Household Credit Repayment Incidents (FICP), the Caisse des Dépôts et Consignations, independent administrative authorities or dispute resolution bodies to comply with their requests;
- companies that conduct business or market studies for us;
- any other person involved in litigation with respect to a transaction;
- the French government, the judicial or administrative jurisdictions/authorities.

#### **Sharing aggregated or anonymised data:**

If we have made your data anonymous, we may share it outside the HSBC Group with partners such as research groups, universities, advertisers or related sites. For example, we may publicly share information to present trends in the overall use of our services. These data do not allow you to identify yourself.

#### **How long do we keep your data?**

We will retain your data as long as you use our services and platforms (e.g. our website or our mobile apps). We may also retain them even if you choose not to use our services or platforms, including to comply with applicable law, to defend our interests, or to enforce our rights. We will not keep your data for longer than necessary, and when we no longer need your data, we will destroy them safely in accordance with our internal policy, or we will make them completely anonymous.

Certain data may be retained for an additional period of time for the management of claims and/or litigation as well as to meet our legal or regulatory obligations or to respond to requests from authorised authorities.

The accounting data may be kept for a period of ten (10) years in accordance with the applicable regulations.

## **[Appendix 2: retention periods by category of purpose]**

### **International data transfers**

Your data are likely to be transferred to, hosted in or accessed from a country located outside the European Union where the data protection laws are not equivalent to those of France or the European Union. We will only make such transfers of data to fulfil the terms of a contract between yourself and HSBC, fulfil a legal obligation, protect the public interest, and defend our legitimate interests.

When data about you are transferred to a country outside the European Union, we will always make sure that they are protected. To this end, we submit all transfers of your data to appropriate and relevant safeguards (such as encryption and contractual commitments, including the entry into standard contractual clauses approved by the EU).

You can obtain further information on how we transfer your personal data outside the European Union by contacting us directly: see the section “More details about your data”.

### **Your rights**

You have rights to your personal data:

- the right to obtain information about the data we hold about you and the processing used;
- in certain circumstances, the right to withdraw your consent to the processing of your data at any time (please note that we may continue to process your personal data if we have a legitimate reason to do so);
- in certain circumstances, the right to receive data in electronic form and/or to ask us to transmit such information to a third party where technically possible (please note that this right only applies to the data you have provided to us);
- the right to modify or correct your data;
- the right to request the deletion of your data in certain circumstances (please note that legal or regulatory provisions or legitimate reasons may require us to retain your data);
- the right to ask us to restrict or oppose the processing of your data in certain circumstances (please note that we may continue to process your personal data if we have a legitimate reason to do so).

You can exercise your rights by contacting us. For this, please refer to the “More details about your data” section. You can find more information about your rights on the CNIL website: <https://www.cnil.fr/>. You also have the right to file a complaint with the National Data Protection Authority (please [click here](#) or send a letter to the following address: CNIL – 3 Place de Fontenoy - TSA 80715 - 75334 Paris - Cedex 07).

### **Client credit check:**

If you wish to open an account or apply for a loan or credit, we may obtain information about you from Banque de France that will be used to determine what type of products and services we can provide you and how much you are able to borrow and repay. We may also carry out other checks on your creditworthiness throughout our contractual relationship.

If you request the opening of a joint account or a loan or credit with another person (for example, your spouse, a family member or anyone sharing your life), we will do the same type of processing on these people.

## **What do we expect from you?**

You must ensure that the information that you have sent us is relevant and up to date. You must also notify us immediately of any significant change in your situation. If you provide us with information on a third party, you must ensure that it is in agreement with this.

## **How do we ensure the security of your data?**

We implement technical and organisational measures to protect your data, including encryption, anonymisation and the implementation of physical security procedures. We require our staff and all third parties working for HSBC to adhere to high standards of security and information protection, including contractual obligations under which they undertake to protect all data and enforce strict data transfer measures.

## **Learn more about your data**

If you would like to know more about the provisions of this Data Protection Policy or contact our Data Protection Officer, you can write to us at the following addresses:

**HSBC Continental Europe — Délégué à la Protection des Données  
38 avenue Kléber — 75116 Paris**

**You can exercise your rights by writing to the following addresses:**

**HSBC Continental Europe** (including HSBC Private Banking)  
Direction de l'Expérience Client - 38 avenue Kléber - 75116 Paris

**HSBC REIM France** – Gestion des Associés  
Immeuble Cœur Défense  
110 Esplanade du Général de Gaulle  
92400 Courbevoie

**HSBC Assurances Vie (France)**  
Immeuble Cœur Défense  
110 Esplanade du Général de Gaulle  
92400 Courbevoie

For the specific case of health data:  
**CBP** - CS 20008 - 44967 Nantes Cedex 9

This Data Protection Policy is subject to change, and the latest applicable version is available at the following address: <https://www.hsbc.fr/1/2/hsbc-france/charte-de-protection-des-donnees>.

## **APPENDIX 1: FOR WHAT PURPOSES DO WE USE YOUR DATA?**

- 1. Supply of products and services, processing of your transactions and execution of your instructions:** we use your data to provide you with products and services and to process your transactions. This includes any entry into, management and execution of all contracts between HSBC and you.  
This processing may be based on our legitimate interest, a legal obligation and/or the performance of any contract with you and/or any commitment made by you or by HSBC.



- 2. Assistance in banking operations:** we use your data to enable and simplify the provision of our banking products and services in accordance with applicable laws and regulations and the rights and interests of our clients. We use them in the provision of administrative services, accounting, business management and IT infrastructure and to evaluate the effectiveness of these services in accordance with applicable regulations and laws and the rights and interests of our clients.

This processing may be based on our legitimate interest, a legal obligation and/or the performance of any contract with you.

This processing may be based on the respect of a legal obligation, the public interest or our legitimate interest.

- 3. Prevention and detection of crime:** we use your personal data to take action to prevent crimes and other offences, including monitoring and fraud risk management, client controls, name and transaction filtering, and potential risk presented by a client. This risk assessment processing is based on compliance with our legal obligations, the public interest and/or our legitimate interest. We may also share your data with the relevant judicial authorities and any other third parties if expressly permitted by law for the purposes of crime prevention or detection. In addition, we may, in conjunction with other financial institutions, take steps to facilitate the prevention of financial crime and risk management if the public interest so requires or if HSBC has a legitimate interest in doing so.

We remain liable to use your personal data for the purposes described above even if you exercise your right to restriction or opposition. This could include:

- Filtering, blocking and analysing payments, instructions or communications that you send or receive;
- The control of the payee of a payment or the issuer of a payment to you;
- The cross-referencing of your personal data that we hold with data held by other HSBC entities;
- The verification that the identity of the persons or companies to whom you make payments or who makes payments to you is accurate and that these persons and companies are not subject to sanctions.

- 4. Security and continuation of our activities:** we take steps to facilitate the continuation of our activities and to ensure the security of the data we hold (including physical security measures) in order to fulfil our legal obligations and to define and put into practice our internal risk strategy in line with our legitimate interest. We also put in place security measures to protect our staff and premises (including a video surveillance device and tracking any incivilities).

- 5. Risk management:** we use your personal data to measure, detect and reduce the likelihood (i) of the occurrence of a financial loss, (ii) harm to our reputation, (iii) the commission of an offence, (iv) a compliance problem or (v) loss problem for a client. This includes credit, commercial, operational and insurance risks (involving the collection and use of health data). Depending on the products and services you receive, your data may be used to detect any risk of market abuse.

We also use them to fulfil our legal obligations and if we have a legitimate interest.

- 6. Online banking, mobile applications and other online product platforms:** when you use HSBC's online platforms and mobile applications, we use your data to make them available to you. These platforms may also allow you to communicate with HSBC.

The legal basis for the use of your personal data for this purpose is contractual.



- 7. Improvement of products and services:** we will use the analysis of your data to identify possible improvements to our products and services (in particular, their efficiency and profitability).  
The legal basis for processing your data for this purpose is our legitimate interest.
- 8. Cookies:** when you use online applications, we will ask you to consent to the use of “cookies”. The legal basis for processing your data for this purpose is your consent.  
Please click [here](#) to learn more about cookies
- 9. Analysing data for client targeting purposes:** we may use your data for analysis to identify opportunities to promote our products and services to current or potential clients. This may include analysing a client’s transaction history to provide tailored and customised products and services.  
This use of the data is based on our legitimate interest.
- 10. Marketing:** we use your data to provide information about HSBC products and services and the products and services of our partners and other third parties. This use of your data is based on our legitimate interest and/or your consent.  
Please see our [Marketing and market research section above](#) for more information on how we use the data for marketing purposes and to learn about your rights in this area.
- 11. Protection of our rights:** we may use your data to protect our rights, including in the defence or protection of legal rights and interests (by recovering amounts owed, assigning receivables, defending our rights intellectual property), lawsuits, claims management or litigation, corporate restructuring or other mergers or acquisitions. We will use them on the basis of our legitimate interests.