In this Data Protection Policy ("Policy"), "Societe Generale", "SG", "we", "us" and "our" refer to "Societe Generale", a public limited company with a capital of €1,000,395,971.25 as of September 23, 2024, registered with the Trade and Companies Register under the unique identification number 552 120 222 and domiciled at 29, boulevard Haussmann 75009 Paris.

About this Policy

Societe Generale, as a banking institution and insurance broker (registered with ORIAS under number 07022493), builds strong and lasting relationships with its clients, based on mutual trust. SG is a brand of Societe Generale.

In order to maintain this trust, we make the security and protection of your personal data an unconditional priority.

With this in mind, Societe Generale complies with all applicable French and European regulations relating to the protection of personal data, in particular the General Data Protection Regulation (EU) 2016/679.

As controller of your personal data, we inform you in particular about the types of personal data we collect, the processing we carry out and the reasons for which we carry them out, as well as about your rights and the contacts or remedies available to you.

This Policy is addressed to and applies to clients and prospects of Global Banking and Investor Solutions with potential business relationships, as well as to persons in contact with our clients when justified (e.g. beneficiary of a transfer, corporate officers, customers and employees of our business partners, etc.) hereinafter referred to as "you/ your".

In particular, it addresses:

1. The types of personal data we collect and process;
2. The purposes of the processing
3. The legal bases on which the processing carried out is based;
4. The recipients and categories of recipients of such personal data;
5. Transfers outside the European Economic Area;
6. Your rights regarding your personal data and how to exercise them;
7. The security of your personal data.
8. The tables setting out the purposes of processing, the legal bases, the categories of data processed, and the associated storage periods are set out in the Annex in paragraph 8

This Policy is updated regularly to reflect changes in SG's practices as well as potential changes in the regulations applicable to personal data. We invite you to consult it regularly to be informed of the latest version in force.

The Client undertakes to communicate this Policy to the persons whose personal data it may be required to provide to Societe Generale.

1. Types of personal data we collect and process

SG collects and processes the following types of personal data:

- **Civil status and identification data:** surname, first name(s), gender, date of birth, copies of identity documents, copies of signatures, etc.;
- **Contact details:** postal addresses, email addresses, phone numbers, etc.
- **Data related to your personal situation:** family situation, matrimonial regime, number and age of children, etc.;
- **Data related to your professional situation:** position held, name of the employer, place of work, etc.;
- **Economic and financial information:** income, financial and tax situation, etc.;
- **Data of banking operations and transactions:** nature of the transactions, date, card payments, transfer, direct debit, amount, denomination, etc.;
- **Connection data related to the use of our online services:** identification and authentication data for your connected spaces, logs, cookies, browsing data on SG sites and applications (SG Markets, Sharinbox, Esalia, etc.);
- **Data processed as part of the electronic signature:** signer's identification data, timestamp, logs, etc.
- **Data from correspondence and communications between you and us, whether face-to-face or remote:** interviews, phone calls, email messages, instant messaging, social media communications or any other type of communication;
- **Data related to the products and services subscribed to:** type of product, payment method, maturity, amount, etc.;
- **Special categories of personal data and personal data relating to criminal convictions or offences.**

This personal data is collected either directly from you or, if necessary, indirectly and lawfully (i) from companies in the Societe Generale Group; (ii) from the Banque de France; (iii) from the National Directory for the Identification of Natural Persons; (iv) from the Directorate General of Public Finances, (v) or more generally from public sources relevant to the various purposes described in paragraph 2.

Finally, where relevant, some of the data or types of data mentioned above may be associated in order to better meet the purposes described in paragraph 2. These associations are always carried out ensuring we only use the data that are strictly necessary to achieve the purpose pursued by the processing (in application of the "minimization" principle provided for by the Regulation) and in a way compatible with the purposes of the carried-out processing.

2. Purposes of processing and retention period of personal data

The personal data referred to in the previous paragraph are processed, depending on the situation, to meet different purposes or goals. We only keep your personal data for as long as necessary to achieve the purposes for which we process it, which may also depend on the periods set by law or by other regulations that are binding on Societe Generale, and in particular the applicable limitation periods.

Personal data collected and processed in accordance with the above-mentioned purposes may also be kept for an additional period if the defense of a right or an interest requires it, or in order to meet the requirements of the competent authorities such as a public authority, a French or international regulator. In this case, the personal data will not be used for other purposes and will only be accessible to authorized persons who need to know it (e.g., legal department, compliance department, audit and inspection body).

Each of these purposes is associated with a type of personal data, a retention period for this data beyond which it is no longer used and is anonymized and/or deleted, except for some of them which may be archived with restricted and secure access, for a specific period.

The different purposes that lead us to process your personal data are as follows:

- To ensure compliance with requirements resulting from the law or regulations to which we are subject, or from supervisory authorities and regulators, regarding in particular *Know Your Customer* (*KYC*) requirements;
- To ensure the proper management of our business relationship with you and to improve the customer experience;
- To finance your projects and provide you with products and services that are adapted to your needs or requests, in connection with your activities and your choices of development;
- To manage the risks we face in the course of our activities and to ensure the necessary controls in this regard.

For these purposes, your personal data may be shared between Group entities.

As part of our activities and our relationship with you, we may use artificial intelligence tools to support the completion of certain tasks (e.g. text generation with human intervention, assistance in the production of translations or summaries, etc.). The data processing carried out in this context are part of an overall purpose of improving customer satisfaction.

You will find the necessary information regarding these purposes and the details of the corresponding processing in the tables in paragraph 8 of this Policy.

3. Legal bases for our processing

3.1.General rules

The processing carried out by SG involving your personal data are based on one of the following legal bases:

- The performance of a contract;
- Compliance with SG's legal and regulatory obligations (e.g. FATCA/CRS);
- Consent;
- Protect the vital interests of the data subject or of another natural person.

3.2.Legitimate interest

The choice of that legal basis is made after a balance made between the interests pursued by SG and the data subjects' interests and an assessment of reasonable expectations in this regard. In addition, suitable safeguards will be put in place to preserve the interests, rights and fundamental freedoms of individuals (information of individuals, right to object and security measures in particular).

Pursuant to this Policy, the legitimate interests pursued by Societe Generale for the processing of your personal data are the following:

- Ensure the security of infrastructures and transactions, prevent the risks of banking systems failure,
- Prevent fraud, fight against money laundering, terrorism financing and cybercrime, comply with regulations relating to international sanctions and embargoes,
- Ensure compliance with local regulations to which the Group is subject given its activities and/or in the countries where Societe Generale is established, meet the requirements and recommendations of authorities and regulators, including outside Europe,
- Assess and manage financial risks, including credit risk, market risk and operational risk, and ensure the effectiveness of internal controls,
- Improve our customers' experience and satisfaction, optimize our operational efficiency and reduce our response times, for example through the development of new offers adapted to the market or the organization of events,
- Develop our products and services with a constant logic of improvement, send relevant marketing communications on products and services that may interest you and meet your needs, particularly in the context of market research,
- To be able to defend ourselves or exercise our rights in court in the event of litigation.

Legitimate interest is also the legal basis for the processing of personal data of customers and employees of our business partners, in the context of the performance of the contracts we have concluded with these legal entities.

4. Categories of data recipients

Your data may be communicated, depending on the purposes pursued:

- To the entities of the Societe Generale Group, its partners, brokers, intermediaries and insurers, subcontractors and service providers. This communication is only made in the context of processing that pursues one of the purposes described in paragraph 2;
- In compliance with the applicable regulations, to third parties in France or abroad for the purpose of establishing, safeguarding or defending a legal claim, in the context of administrative or criminal investigations by one or more regulators, compliance with commitments made to them or in the context of legal disputes of any kind;
- To certain regulated professions such as auditors in order to provide regulatory reports or lawyers, to act in defense of SG's interests and rights;
- To payment initiators and account information service providers (aggregators), only if you consent to this or at your request.

5. Transfers outside the European Economic Area

Due to the international dimension of the Societe Generale Group, the processing listed in paragraph 8 below may involve transfers of personal data to countries that are not members of the European Economic Area (EEA), of which personal data protection laws differ from those of the European Union.

In particular, your personal data may, within the limits of what is permitted by the applicable regulations, be communicated to official bodies and to the competent administrative and judicial authorities of non-EEA countries, in particular in the context of regulations on anti-money laundering and terrorist financing, international sanctions and embargoes, the prevention of fraud and the determination of your tax status.

When transferring personal data to countries outside the EEA, a precise and demanding legal framework governs this transfer, in accordance with the applicable European regulations, especially through the signing of Standard Contractual Clauses established by the European Commission. In addition, appropriate and additional security measures may be put in place to ensure the protection of personal data transferred outside the EEA. The Standard Contractual Clauses are available on the CNIL website (www.cnil.fr). For more information, you can send your request to the contact address given in paragraph 6.

To find out more about the specific case of transfer instructions transmitted between banks via secure international interbank telecommunications networks, please consult the "Swift Information Notice" on the fbf.fr website.

6. Your rights

You have a right of access to your personal data as well as a right to rectification, erasure, limitation of processing, as well as a right to the portability of some of your data. You may also withdraw your consent at any time when this legal basis applies to the processing, or object to the processing of your personal data on grounds relating to your particular situation, or set general or specific guidelines on the use of your personal data in the event of death.

You may also, at any time and free of charge, without having to justify your request, object to your personal data being used for marketing purposes. If your objection request does not concern commercial communications, SG may refuse to follow up on your request if:

- There are legitimate and compelling grounds for processing personal data or the personal data is/are necessary for the establishment, exercise or defense of legal claims;
- You have consented to the processing of your data, in which case you must withdraw this consent and not object;
- The processing in question is necessary for the performance of a contract between you and Societe Generale;
- We have a legal obligation to process your personal data;
- The processing is necessary to protect the vital interests of the data subject or of another natural person.

You can exercise your rights and/or contact the Personal Data Protection Officer by email:

- For financing, market, transactions (banking, commercial and corporate transactions) and/or payments at the following address: FR-GDPR-SG-CONTACT@sgcib.com;
- For Securities and Employee Savings Services activities at the following address: SGSS-PersonalData@socgen.com

Finally, you have the right to lodge a complaint with the Commission Nationale de l'Informatique et des Libertés (CNIL), the supervisory authority in charge of compliance with personal data obligations in France.

7. The security of your personal data

SG takes all physical, technical and organizational measures to ensure the confidentiality, integrity and availability of personal data, in particular to protect it against loss, accidental destruction, alteration and unauthorized access.

In the event of a personal data breach, resulting in a risk to the rights and freedoms of natural persons, SG will notify the breach to the CNIL in compliance with the regulatory deadline.

If this personal data breach presents a high risk to the rights and freedoms of natural persons, SG will inform you as soon as possible of the nature of this breach and the remedial action taken.

8 Appendix

Macro-Purpose 1: Compliance with legal and regulatory requirements			
Sub-purpose/processing concerned	**Legal basis**	**Data categories**	**Retention period**
Anti-Money Laundering and Terrorism Financing/Compliance with International Sanctions and Embargoes *This processing involves the collection and analysis of data in order to verify the identity of stakeholders, assess the risks associated with financial transactions, detect illicit activities and ensure compliance with regulations on international sanctions and embargoes. Compliance with these obligations is an integral part of Know Your Customer (KYC) process*	Legal/regulatory obligation Legitimate interest	Identification data Contact details Financial data Special categories of data and data relating to criminal convictions or offences	Until the end of the customer relationship and for a maximum additional period of **5 years** or **10 years**, depending on the limitation period and the law applicable to the data concerned
Market Abuse detection *Implementation of systems for the prevention, monitoring, detection and reporting of market abuse*	Legal/regulatory obligation	Identification data Contact details Financial data Communications data Personal situation data	For a maximum period of **10 years** from the date of the operation concerned
Communication recording *relating to the receipt, transmission, execution of orders or in order to establish proof of contractual formation...*	Legal/regulatory obligation	Identification data Contact details Communication data	For a maximum period of **5 years** from the date of the operation concerned
Tax transparency *Management of clients' taxation, fulfilment of reporting obligations according to tax residence, search for indicators of Americanness (so-called FATCA legislation) ...*	Legal/regulatory obligation	Identification data Contact details Financial data	For a maximum period of **10 years** from the date of the operation concerned
Prevention of conflicts of interest and corruption/business ethics *Prevention and detection of corruption and influence peddling, implementation of actions and obligations arising from the "Sapin 2" law, procedures to detect the risks of conflicts of interest and limit the related risks...*	Legal/regulatory obligation	Identification data Contact details Financial data	Until the end of the customer relationship and for a maximum additional period of **5 years**
Client Protection *Establishment of measures to comply with laws and regulations related to customer and consumer protection.*	Legal/regulatory obligation	Identification data Contact details Financial data	Until the end of the customer relationship and for a maximum additional period of **5 years**

Macro-Purpose 2: Commercial relationship management			
Sub-purpose/processing concerned	**Legal Basis**	**Data categories**	**Retention period**
Commercial relationship management *Promotional operation of products and services, development of relationships with existing or potential customers, companies or financial institutions, updating of the customer database...*	Legitimate interest	Identification data Contact details Professional data	Until the end of the customer relationship and for a maximum additional period of **5 years**
Event planning *Webinars, meetings & conferences*	Legitimate interest	Identification data Contact details	**3 years** from the end of the event and for a maximum additional period of **5 years**
Management of authorizations and access rights *Allowing access to platforms, management of the customer area, management of mandates and powers, etc.*	Legitimate interest	Identification data Contact details Professional data Connection data related to the use of our online services	Until the end of the customer relationship and for a maximum additional period of **3 years**
Complaint management and customer satisfaction improvement *Answer customer complaints and management of claims or disputes, effective follow-up to ensure,...*	Legal/regulatory obligation Legitimate interest	Identification data Contact details Business data Communications data Connection data related to the use of our online services	Until the end of the customer relationship and for a maximum additional period of **5 years**

Macro-Purpose 3: Provision of banking services			
Sub-purpose/processing concerned	**Legal Basis**	**Data categories**	**Retention period**
Global Transaction and Payment Services *Payment and Cash Management, Trade Finance, International Payments, Correspondent Banking*	Legitimate interest Legal/regulatory obligation	Identification data Banking operations and transactions data Business data	Until the end of the customer relationship and for a maximum additional period of **10 years**
Corporate Finance Services *Financing, Financing Advisory, Mergers & Acquisitions, Client Coverage, Securitization*	Legitimate interest	Identification data Contact details Economic and financial information Data from correspondence and communications	Until the end of the customer relationship and for a maximum additional period of **10 years**
Securities Services Activities *Issuer Services, Securities Custody, Fund Transactions, Fund Administration*	Legitimate interest Performance of the contract	Identification data Contact details Data related to the products and subscribed services Professional data	Until the end of the customer relationship and for a maximum additional period of **5 years, 10 years, or 30 years** depending on the applicable law
Employee savings *Account keeping of retirement and employee savings schemes*	Legitimate interest Legal/regulatory obligation	Identification data Contact details Business data Connection data related to the use of our online services Financial data	Until the end of the customer relationship and for a maximum additional period of **10 years** Or **30 years** *old (supporting documents related to employee savings operations)*
Market activities *Market operations (trade, sale, structuring, negotiation, etc.)* *Research and data analysis on the capital markets "Cross Asset Research"*	Legitimate interest	Identification data Contact details Professional data Data related to the products and services subscribed to	Until the end of the customer relationship and for a maximum additional period of **10 years**

Macro-Purpose 4: Risk management			
Sub-purpose/processing concerned	**Legal Basis**	**Data categories**	**Retention period**
Credit risk management *Anticipation of the risk resulting from the inability of customers or other counterparties to meet their financial commitments*	Legal/regulatory obligation Legitimate interest	Identification data Contact details Financial data Banking and transaction data	Until the end of the customer relationship and for a maximum additional period of **10 years**
Internal control *Management of the risks of non-compliance in compliance with the regulatory obligations of the banking sector (e.g. permanent or periodic audits, etc.)*	Legal/regulatory obligation Legitimate interest	Identification data Contact details Professional data Connection data related to the use of our online services Financial data Banking transaction and transaction data	Until the end of the customer relationship and for a maximum additional period of **10 years**
Operational Risk Management and Cybersecurity *Computer Network Security, Internal Oversight and Control, Transaction Security and Security of International Payment Networks, Strong Authentication and IT Logs*	Legitimate interest	Identification data Contact details Professional data Communications data Connection data related to the use of our online services	Until the end of the customer relationship and for a maximum additional period of **5 years** **Or 6 months** for computer logs
Fraud prevention *Prevent, detect and manage fraud through transaction monitoring and identification of perpetrators of acts classified as attempted fraud or proven fraud*	Legitimate interest	Identification data Contact details Professional data Connection data related to the use of our online services Financial data Banking transaction and transaction data	Until the end of the customer relationship and for a maximum additional period of **10 years**