PRIVACY POLICY
SOCIETE GENERALE LUXEMBOURG

PRIVACY POLICY JANUARY 2025

C'EST VOUS L'AVENIR

SOCIETE GENERALE

ABOUT THE PRIVACY POLICY

Societe Generale Luxembourg ("SG Luxembourg, or the "Bank" or "we"), is a multi-business bank with a private banking, corporate services and securities services activity (authorized as a credit institution under Luxembourg law by the CSSF on the basis of the law of 5 April 1993 relating to the financial sector as it has been amended). SG Luxembourg belongs to the Societe Generale Group ("Societe Generale").

SG Luxembourg has always built strong and lasting relationships with its clients and partners, based on mutual trust and mutual interest. To maintain this trust, we make the security and protection of your data an unconditional priority

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

In our capacity as the controller of your personal data, we would like to inform you in particular about the types of personal data we collect, the processing we carry out and the reasons why we carry it out, as well as about your rights and the contacts or remedies made available to you

This Policy is intended for and applies to clients and prospects of Societe Generale Luxembourg with, potential business relationships, as well as natural persons involved in a relationship with a client such as an agent, a legal representative, a guarantor, a designated contact, an agent or a beneficial owner and its partners (e.g. beneficiary of a transfer, corporate officers, clients and employees of our business partners, etc.) hereinafter referred to as "you/your".

In particular, it addresses:

1. Data controller;
2. The types of personal data we collect and process;
3. The goals of the treatment process;
4. The legal bases on which the processing carried out is based;
5. The recipients and categories of recipients of yourthis personal data;
6. The retention periods of your personal data;
7. Transfers outside the European Economic Area;
8. The security of your personal data;
9. Your rights regarding your personal data and how they are exercised;
10. The tables containing the purposes of processing, the legal bases, the categories of data processed and the associated retention periods are set out in the Annex.

Cette Politique est mise à jour régulièrement pour refléter les évolutions des pratiques de SG ainsi que les potentielles évolutions de la réglementation applicable aux données personnelles. Nous vous invitons à la consulter régulièrement pour être informés de la dernière version en vigueur.

Thsis Privacy Policy supplements the General Terms and Conditions applicable to Societe Generale Luxembourg products and services (General Terms and Conditions) and its appendix (outsoursing summary table).

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

1. DATA CONTROLLER

Your personal data are processed by Societe Generale Luxembourg, a limited company registered with the Luxembourg RCS under the number B6061 and having its registered office at 11, Avenue Emile Reuter, L-2420 Luxembourg. Tel. : (+352) 47 93 11 1 Fax. : (+352) 22 88 59.

The Bank - in its capacity as data controller - ensures that the necessary provisions are made regarding compliance with the legal requirements regarding personal data.

2. WHAT TYPES OF PERSONAL DATA ARE PROCESSED AND WHERE DO THEY COME FROM?

SG Luxembourg collects and processes various data about you, including in particular:

- **Civil status data and identification data:** surname, first name(s), gender, date of birth, nationality, identity documents, examples of signatures, possible legal protection measure (safeguard of justice, curatorship, guardianship) etc.;
- **Contact details:** postal addresses, e-mail addresses, telephone numbers, etc.;
- **Data related to your personal situation:** family situation, matrimonial regime, number and age of dependent children, center of interest;
- **Data related to your professional situation:** professional status, position, job title, employer name, workplace, etc.;
- **Economic and financial data:** data on banking transactions and transactions (nature of transactions, date, card payments, transfer, direct debit, amount, wording, etc.), data related to the products and services subscribed (type of product, method of settlement, maturity, amount), tax residence and country of residence, account number, credit card number, amount of income, tax brackets, valuation of assets;
- **Data, ratings and ratios** relating to your investor or borrower profile and other data necessary for sound risk management of the Bank in accordance with the law;
- **Data from correspondence and communications between you and us,** in branches or remotely (interviews, telephone calls when recorded, electronic messages, instant messaging, communications on social networks or any other type of communication);
- **Login data related to the use of our online services:** identification and authentication data at your connected spaces, logs, cookies, navigation data (IP address in particular) on Societe Generale websites and applications;
- **Data processed as part of the electronic signature:** signatory identification data, time stamp, logs, etc.
- **Data from video surveillance.** .
- **Specific categories of personal data** and personal data relating to criminal convictions or offenses.

Your personal data are collected either directly from you, in particular when we present you with services and/or products, during the process of entering into a relationship or as part of the customer relationship or, if necessary, indirectly (i) generated by your banking and insurance activities; (ii) obtained from a third-party and / or public source (e.g. public authorities or institutions, institutions operating professional databases, other financial institutions, fraud prevention bodies, or data providers), in accordance with data protection regulations and with regard to the various purposes described in paragraph 3.

Finally, where relevant, some of the data or categories of data mentioned above may be reconciled in order to better fulfill the purposes described in paragraph 3. These reconciliations are always made by ensuring that only data strictly necessary to achieve the purpose of the processing (in application of the principle of “minimization” provided for by the regulations) are used.

3. THE OBJECTIVES PURSUED BY THE PROCESSING (PURPOSES)

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

It is specified that the personal data collected and processed in accordance with the purposes listed below may be kept for an additional period if the defense of a right or interest so requires, or in order to meet the requirements of the authorized authorities such as, for example, a public authority, or a regulator (Luxemburgish or international). In this case, the personal data will not be used for other purposes and will be accessible only to authorized persons who need to know them (examples: legal service, compliance service, audit and inspection corps).

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

The different purposes that lead us to process your personal data are the following:

- **To ensure compliance with the requirements resulting from the law or regulations to which we are subject, or from supervisory authorities or regulators, regarding in particular *Know Your Customer* (KYC) requirements;**
- **To ensure the proper management of our commercial relationship with you and improve the customer experience;**
- **To provide you with products and services tailored to your needs or requests, in line with your activities and development wishes;**
- **To manage and control the risks we face in our operations.**

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

As part of our activities and our relations with you, we may use artificial intelligence tools to support the performance of certain tasks (e.g. generating texts with human intervention, helping with translation or summaries, etc.). The data processing carried out in this context is part of an overall aim of improving customer satisfaction.

You will find the necessary information regarding these purposes and the details of the corresponding processing operations in the tables in paragraph 10 of this Policy.

How SG Luxembourg determines the products and services that correspond to your situation or profile?
The Bank determines which products and services may be suitable for you based on:

- Market segmentations to suggest innovative services and products that best meet your needs;
- Classifications required by the regulations in force (AML, DAC, FATCA, etc.);

The Bank uses the above processing as decision support, but does not implement any automated decision-making process that produces legal effects for the data subjects. Human intervention is always part of the decision-making process.

4. THE LEGAL BASIS FOR PROCESSING

1. GENERAL PROVISIONS

The processing carried out by Societe Generale Luxembourg involving your personal data are is based on one of the following legal bases:

- **Contractual or pre-contractual performance (e.g. management of accounts, execution of services and products contracted)**
- **Compliance with legal and regulatory obligations incumbent on Societe Generale Luxembourg (example: combating money laundering and terrorist financing,);**
- **Consent.**

2. LEGITIMATE INTEREST

The choice of this legal basis is made after balancing the interests pursued by SG against the interests of the data subject and the assessment of reasonable expectations in this regard. In addition, safeguards are put in place to safeguard the interests, rights and fundamental freedoms of individuals (in particular information of individuals, right of opposition and security measures).

In accordance with this Policy, Societe Generale's legitimate interests in the processing of your personal data are as follows:

- **Ensure the security of infrastructure and transactions,** preventing the risks of banking system failure,
- **Prevent fraud, fight against money laundering,** terrorism financing and cybercrime, comply with regulations relating to international sanctions and embargoes
- **Ensure compliance with the local regulations to which Societe Generale Luxembourg is subject** given its activities and/or in the countries where it 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 effective 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 in a continuous improvement logic,** send relevant marketing communications on the products and services likely to interest you and correspond to your needs, particularly in the context of market studies,
- **To be able to defend ourselves or exercise our rights in court in the event of disputes.**

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

5. WHO ARE THE RECIPIENTS OF THE PROCESSED DATA?

SG Luxembourg is bound by professional secrecy and may only share your personal data under strict conditions or with your consent.

The Bank may be required to communicate your personal data, depending on the purposes pursued:

- **To certain Societe Generale group entities** notably in the context of the pooling of Societe Generale group resources and services (e.g. consolidated risk management);
- **To Independent agents, intermediaries or brokers financial institutions, financial and commercial partners** with whom we have regular relationships (e.g. banks, insurance companies, debit and credit card issuers);
- **To official bodies, regulators and administrative, financial, tax or judicial authorities, located in or outside the European Economic Area,** on request and within the limits authorized by the applicable regulations, in particular in the context of the fight against money laundering and the financing of terrorism, international sanctions and embargoes, the fight against fraud and the determination of your tax status;
- **To certain regulated professionals such as lawyers, notaries or auditors;**
- **To the Bank's intermediaries in banking operations, in particular international payment systems and/ or bank correspondents, located in or outside the European Economic Area when executing transfers and SEPA domiciliations (including the related messages) in the name and on behalf of the Client.** International payment systems and/or correspondents require the identification of the payer and the payee. Accordingly, the Bank is obliged to identify the Client as the originator in the transfer documents and to disclose Client-related Information in these documents;
- **To the Bank's subcontractors and service providers solely for the purposes of the services to be performed on its behalf** and in particular the provision of banking and financial services or products or the performance of surveys or statistics;
- **The Bank is also required to share your data when professional secrecy is waived by law and in particular with regard to tax administrations and supervisory authorities (CSSF, CNPD, etc.)** Secrecy cannot be invoked against a judicial authority acting in criminal proceedings, or in civil proceedings where a specific text expressly provides for it.

6. WHAT ARE THE RETENTION PERIODS FOR YOUR DATA?

The personal data referred to in paragraph two are processed, depending on the situation, in order to meet different objectives or purposes. Each of these purposes is associated with a category of data, a data retention period beyond which they are no longer being used, archived then anonymized and/or deleted.

The retention period of your data depends on the nature of the data, the purposes pursued to which are added the retention periods imposed by applicable legal and regulatory provisions.

The Bank keeps your data for the longest period required by applicable regulations. The deadlines may also be extended in the event of legal action. In this case, the data is kept until the end of the legal proceedings and then archived according to the applicable legal limitation periods. When personal data are collected for several purposes or when several legal and regulatory provisions are cumulatively applicable, it is kept until the longest retention or archiving period has expired.

Different retention periods apply, in particular concerning:

- **Customer data,** most of the information is kept for the duration of the contractual relationship and for ten years after the end of the contractual relationship;
- **Data collected for pre-contractual purposes,** without the effective conclusion of a contract: When you have contacted the Bank for a request for a product or service or for a simulation and your request has not been followed by a subscription, the Bank keeps your data in order to be able to reissue a simulation or keep a record of the advice that she was brought to provide you. These data are kept for a period of five years or more, if the competent authorities so require, for the purposes of combating money laundering and the financing of terrorism and the fight against fraud as from their collection.

7. TRANSFERS OUTSIDE THE EUROPEAN ECONOMIC AREA

Given in particular the international dimension of SG Luxembourg, certain processings are likely to involve transfers of personal data to countries which are not members of the European Economic Area (EEA), which data protection laws differ from those of the European Union. In this case, unless the country concerned has been officially recognized by the European Commission as guaranteeing an adequate level of protection of personal data, the Bank will ensure that the personal data transferred are protected by appropriate standard contractual clauses or other guarantees mentioned by the GDPR.

In particular, your personal data may, within the limits of what is authorized by the applicable regulations, be communicated to official bodies and to the authorized administrative and judicial authorities of countries which are not members of the European Economic Area (EEA).

Thus, the Bank will be able, in accordance with the law, to disclose certain data in the context of the automatic exchange of tax data, which obliges the Bank to declare to the “Administration des Contributions Directes” (“ACD”) du Luxembourg the required information, in particular the identity, account numbers, balances and banking income of the customer not residing in Luxembourg but in another country participating in the international exchange of tax information, with a view to their transmission to the competent authorities of the country of residence of the customer, including when the country concerned does not ensure a level of protection of personal data equivalent to that of European legislation.

In addition, the personal data included in / or accompanying certain transactions, including in particular fund transfers (payment or direct debit orders) are processed by the Bank and by other specialized companies, such as SWIFT (Society for Worldwide Interbank Financial Telecommunication) insofar as they are necessary to execute and document before mentioned transactions. This processing can be carried out in centers located in other European countries and in the United States, in accordance with local legislation. Consequently, the authorities of the countries concerned may request access to personal data held in these operational centers as part of their legal missions, including for the purpose of combating money laundering and the financing of terrorism.

The client who instructs SG Luxembourg to carry out a payment order or any other similar operation expressly instructs the Bank so that the data necessary for the correct execution of the transaction are transferred and processed outside Luxembourg, including when the country concerned does not ensure a level of protection of personal data equivalent to that of European legislation.

In the context of the execution of securities orders by external service providers, respectively the deposit of securities with external service providers having their head office inside or outside the European Union; these may be subject to national laws and regulations (for example in the context of the fight against money laundering respectively the financing of terrorism) or other rules, which require the obtaining of personal data of clients or where applicable from their legal representatives, beneficial owners, final contractors or securities depositors as well as their transmission to the competent judicial or supervisory authorities at national level, to securities issuers or to other third parties involved in the execution of securities orders or the deposit of securities.

For these specific cases, the Bank is obliged to transmit the personal data of clients, their legal representatives, beneficial owners, final contractors or securities depositors to external service providers.

The client, respectively their legal representatives, confirm that they have informed the beneficial owners and any other third party concerned of the Bank's obligations described above, have obtained their mandate and agreement to the transfer and processing of the related data and to transmit it to the Bank upon simple request.

The client, respectively its legal representatives, expressly instruct the Bank, in their own name and on behalf of the beneficial owners and any other third party concerned, in view of the transfer and processing of the data necessary for the correct execution of securities transactions, respectively of the deposit of securities to external service providers in Luxembourg or abroad, and instruct the Bank to proceed with said transfers, even if these countries do not have the level of protection of personal data equivalent to that provided for by European legislation.

When personal data are transferred to countries that are not members of the European Economic Area (EEA), a precise and demanding framework, in accordance with the applicable European regulations, governs this transfer, in particular byby signing standard contractual clauses approved by the European Commission. In addition, appropriate security measures have been put in place to ensure the protection of personal data transferred outside the EEA unless the country concerned has been officially recognized by the European Commission as guaranteeing personal data an adequate level of protection compared to the European standard. The Standard Contractual Clauses are available on the website of the "Commission Nationale pour la Protection des Données" ("CNPD") following this link: SCC EC

For more information, you can send your request to the contact address indicated in paragraph 9.

8. THE SECURITY OF YOUR PERSONAL DATA

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

In the event of a breach of personal data, presenting a risk to the rights and freedoms of natural persons, SG Luxembourg will notify the breach in question to the CNPD in accordance with the regulatory deadline. In the event that this violation presents a high risk to the rights and freedoms of natural persons, SG Luxembourg will inform you as soon as possible of the nature of this violation and the measures implemented to remedy it.

9. WHAT ARE YOUR RIGHTS?

You have the following rights, within the limits and conditions imposed by law:

- **The right to information:** In the hope that this policy will have answered your questions, you can contact the Bank's Data Protection Officer (DPO) for further information.
- **The right to access your data.** You can access your data by contacting the Bank's DPO. Please note, however, that the Bank processes a large amount of data and in accordance with the law, you may be asked to specify, before any provision of data, which data or processing operations your request relates to.
- **The right to rectify** your data when it is incorrect or obsolete.
- **The right to withdraw your consent** if you have given your consent for a processing of your personal data; it should be noted that such withdrawal has no retroactive effect and will not prevent the Bank from continuing lawful processing, in particular those required by law.
- **The right to lodge a complaint with the National Data Protection Commission (CNPD)** when you consider that the processing of your data is not in accordance with the law: by filling in the online form CNPD online complaint form or to print and complete the Complaint form by hand. In this case, please send it to the following address: National Data Protection Commission Complaints Department 15, Boulevard du Jazz L-4370 Belvaux

In certain cases and according to the conditions set by law (in which case the Bank will first check that these conditions are met), you also have the following rights:

- **The right to request the erasure** of your data.
- **The right to request the restriction** of the processing of your data;
- **The right to object** to the processing of your data for prospecting purposes or for any other legitimate reason (except for legitimate and compelling reasons for the Bank to continue the processing).
- **The right to the portability** of the data you have provided to the Bank, to the extent technically possible.

For any questions concerning the processing of your personal data carried out by SG Luxembourg, and for any request relating to the exercise of your rights, you can contact our DPO by email at lux.dpooffice@socgen.com or by post to Societe Generale Luxembourg, DPO, B.P. 1271, L 1012 Luxembourg.

For all your requests please attach a copy of your ID, so that we can identify you. This policy may need to be amended to protect your personal data as much as possible. The latest version is available on the Bank's website https://www.societegenerale.lu/en/legal-information/

10. ANNEX: TABLES CONTAINING THE PURPOSES OF PROCESSING, THE LEGAL BASES, THE CATEGORIES OF DATA PROCESSED AND THE ASSOCIATED RETENTION PERIODS

Below is a table summarizing the purposes.

MACRO-PURPOSE 1: COMPLIANCE WITH LEGAL AND REGULATORY REQUIREMENTS

SUB-PURPOSE/PROCESSING CONCERNED	LEGAL BASIS	CATEGORY OF DATA	RETENTION PERIOD
Enforce banking and financial regulations under which the Bank must, in particular, put in place security measures to prevent abuse and fraud; Detect unusual transactions; Apply vigilance measures with regard to certain categories of persons; Record commercial exchanges; Report certain transactions to the competent authorities; Where the Bank finds a criminal violation, report it to the competent authorities if necessary.	Legal/regulatory obligation	Identification data Contact details Financial data Specific categories of data and data relating to criminal convictions or offenses	Until the end of the customer relationship and for a maximum additional period of **10 years.**
Anti-money laundering/Anti-terrorism/ compliance with International Sanctions and Embargos These processes involve the collection and analysis of data in order to verify the identity of stakeholders, assess the risks related to financial transactions, detect illegal activities and ensure compliance with regulations on international sanctions and embargoes. Compliance with these obligations is an integral part of KYC (Know Your Customer); Respond to official requests from duly authorized public or judicial authorities.	Legal/regulatory obligation Legitimate interest	Identification data Contact details Financial data Specific categories of data and data relating to criminal convictions or offenses	Until the end of the customer relationship and for a maximum additional period of **10 years.**
Detection and treatment of market abuse Implementation of mechanisms 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 operation concerned.
Recording of communication The recording of your conversations and communications, regardless of whatever their medium (e-mails, faxes, telephone interviews, electronic messaging, etc.) may be carried out for the purpose of improving telephone reception, complying with legal and regulatory obligations relating to financial markets, and ensuring the security of the transactions, processing and services carried out.	Legal/regulatory obligation Legitimate interest	Identification data Contact details Communication data	For a maximum period of **10 years** from the date of the communication concerned.
Tax transparency Management of customer taxation, fight against tax fraud (DAC6 legislation), fulfillment of reporting obligations according to tax residence (CRS legislation), search for indications of Americanity (FATCA legislation), etc.	Legal/regulatory obligation	Identification data Contact details Financial data	**10 years** from year-end to which the documents relate.
Prevention of conflicts of interest/fight against corruption/business ethics Prevention and detection of corruption and influence peddling, procedures to detect and mitigate risks of conflicts of interest.	Legal/regulatory obligation	Données d'identification Coordonnées de contact Données financières	Until the end of the customer relationship and for a maximum additional period of **10 years.**
Client Protection Implementation of measures to comply with laws and regulations related to customer and consumer protection (e.g. MIFID).	Legal/regulatory obligation	Identification data Contact details Financial data	Until the end of the customer relationship and for a maximum additional period of **10 years.**

MACRO-PURPOSE 2: COMMERCIAL RELATIONSHIP MANAGEMENT

SUB-PURPOSE/PROCESSING CONCERNED	LEGAL BASIS	CATEGORY OF DATA	RETENTION PERIOD
Management and development of commercial relationship Product and service promotions, development of relationships with existing or potential customers, updating of the customer database; Establishing statistics, models or tests, to optimize risk management, or to improve products and services and develop new ones; Assessing the possibility of offering you a product or service and under what conditions; Promoting products and services that correspond to your situation or profile (this can be done for example by analyzing the products or services you already own or use); Conducting satisfaction surveys and polls.	Legitimate interest	Identification data Contact details Professional data	Until the end of the customer relationship and for a maximum period of **10 years**.
Organization of events Webinar, conferences, meetings Carrying out communication, prospecting and sales promotion operations	Legitimate interest Consent	Identification data Contact details	**10 years** from event end.
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 **10 years**.
Complaint management and improved customer satisfaction Respond to customer complaints and complaints, manage disputes, ensure effective follow-up,	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 **10 years**.

MACRO-PURPOSE 3: PROVISION OF BANKING SERVICES

SUB-PURPOSE/PROCESSING CONCERNED	LEGAL BASIS	CATEGORY OF DATA	RETENTION PERIOD
The Bank uses your data to provide you with services and products and in particular to: provide you with information about its products and services; carry out the operations necessary for the management of the products or services to which you have subscribed.	Performance of the contract	Identification data Contact details Data related to the products and services subscribed Professional data	Until the end of the customer relationship and for a maximum additional period of **10 years**.
Global Transaction and payment services Flow and liquidity management, international payments, bank correspondence; Managing and processing payment incidents, defaults and related amicable and judicial recovery transactions.	Legitimate interest Legal/regulatory obligation Performance of the contract	Identification data Banking transactions and Professional data	Until the end of the customer relationship and for a maximum additional period of **10 years**.
Corporate finance services Financing, financing advisory, 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 **10 years.**
Market activities Market transactions (trade, sale, structuring, trading, etc.)	Legitimate interest	Identification data Contact details Professional data Data related to the products and services subscribed	Until the end of the customer relationship and for a maximum additional period of **10 years.**

MACRO-PURPOSE 4: STEERING RISK MANAGEMENT

SUB-PURPOSE/PROCESSING CONCERNED	LEGAL BASIS	CATEGORY OF DATA	RETENTION PERIOD
Credit risk management Anticipation of risk arising 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 **10 years** **Or 6 months** for IT logs.
Fight against fraud Prevent, detect and manage fraud through transaction monitoring and identification of perpetrators as fraud attempts or actual fraud, Prevent attacks on property and people.	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**.

PRIVACY POLICY
SOCIETE GENERALE LUXEMBOURG
JANUARY 2025

SOCIETE GENERALE