

PRIVACY POLICY



SOCIETE GENERALE AMSTERDAM

As from 25 May 2018
(Updated on 4 December 2024)

PRIVACY POLICY

In this Privacy Policy, “**Société Générale**”, “**we**”, “**us**” and “**our**” means Société Générale’s Dutch branch located at Amstelplein 1, Rembrandt Tower, 1096 HA Amsterdam (with company number 33149169).

About this Privacy Policy

For the purposes of data protection law, we are a data controller in respect of personal data. Société Générale is responsible for ensuring that it uses personal data in compliance with applicable data protection laws, including the General Data Protection Regulation (regulation (EU) 2016/679 - “GDPR”) and the GDPR Implementation Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming*; “UAVG”) in the Netherlands.

This Privacy Policy applies to clients, legal representative or employees of Société Générale’s clients, beneficial owners of Société Générale’s clients and potential business relationships (hereafter referred to together as the “Clients”).

The Clients undertake to notify their representatives and employees (the “Data Subjects”) of this Privacy Policy.

This Privacy Policy sets out the basis on which any personal data that Clients provide to us, that we create, or that we obtain about Clients from other sources, will be processed by us. Please take the time to read and understand this Privacy Policy.

This Privacy Policy includes in particular:

1. The categories of personal data collected and processed
2. The purposes of processing of personal data
3. The legal grounds for processing personal data
4. Communication of personal data to third parties
5. Transfers outside the European Economic Area
6. Retention of personal data
7. Rights of Data Subjects
8. Security of personal data
9. Contacting us

This Privacy Policy may be amended or updated from time to time to reflect changes in practices with respect to the processing of personal data or changes in applicable law.

1. Categories of personal data collected and processed

In the course of its banking relationship with Clients, Société Générale will collect and process the following personal data relating to the Data Subjects:

- Personal details: names, surnames, gender, birth dates and other elements of civil status;
- Identity documents: copy of passport, copy of identity card, example of signature;
- Contact details: work postal addresses, work and private email addresses, professional phone number, job title, scope of delegation;

- Financial details, including IBAN identifier;
- Employment data: work title and information relating to their professional and (where relevant) financial status;
- Data related to electronic identification and data relating to IT usage and website navigation;
- Personal preference such as meals and rooms;
- Access to Société Générale premises
- Content of any electronic communication (e.g. telephone calls and interviews, internet discussion, e-mails, data related to payment systems etc.) exchanged between the Client and us.

Please consult the Annex to this Privacy Policy for a detailed overview of the categories of personal data processed by Société Générale.

These personal data are collected either directly from the Clients, or via companies belonging to the Société Générale Group, or from public sources.

When the personal data are collected from the Clients (including their representatives or employees), the provision of the personal data requested is essential for the provision of products or services by Société Générale. Any refusal to do so may have as a consequence that Société Générale may not be able to provide quality services to the Client or may be in breach of a statutory or regulatory obligation applicable to Société Générale.

2. Purposes of processing personal data

The above personal data will be stored and processed by Société Générale for the following purposes:

- Complying with statutory and regulatory requirements to which Société Générale is subject and managing internal compliance, particularly in matters concerning identification controls, checking transactions, operational risk management, the prevention of conflicts of interests, the prevention and detection of fraud and related crimes, the fight against money laundering and financing of terrorism, regulatory reports and financial communications ;
- Financial management of Société Générale ;
- Management and performance of the contractual relationship between Société Générale and the Client, including onboarding, credit analysis, creation of consolidated risk profile for the Client, implementing an improved client service policy ;
- Management of payment systems & services and associated flows ;
- Management of audit and inspection ;
- Administering and operating account, providing; offering and managing finance and trading products and services, including remote banking ;
- Management of the website of Société Générale's Dutch branch ;
- Business development of corporate prospects and Clients, including marketing, organizing of events and conducting surveys ;
- Security of Société Générale premises ;
- Management of third party services providers and vendors ;

- Management of legal affairs and judicial proceedings ;
- Management of the rights of the data subjects, including for internal statistical purposes.

Furthermore, Société Générale will, in accordance with applicable legal requirements, record electronic communications (phones, e-mails) with its Clients and counterparts. When it occurs, the recording of electronic communication by Société Générale is made for the purpose of establishing proof of transactions or of another professional communication. Data pertaining to electronic communications and the content of said communications may be saved until the end of the period during which the underlying transaction can be legally disputed. The Client undertakes to inform his employees and representatives that any communication with Société Générale must be strictly confidential and professional.

Please consult the Annex to this Privacy Policy or a detailed overview of the purposes of personal data processing by Société Générale.

3. Consequences of not providing

If Société Générale asks you to provide personal information to comply with a legal requirement or to perform a contract with you, we will make this clear at the relevant time and advise you whether the provision of your personal information is mandatory or not (as well as of the possible consequences if you do not provide your personal information). Consequences of not providing the requested information could result for Société Générale in not meeting our legal requirements and not providing the service as intended, as we may not be able to accomplish some or all of the purposes outlined in this Privacy Policy.

4. Legal grounds for processing personal data

The processing of personal data is based on:

- the necessity to perform a contract ;
- a statutory or regulatory requirement ;
- the legitimate interest of Société Générale (see Annex for further details).

Please consult the Annex to this Privacy Policy for a detailed overview of the legal grounds for the processing of personal data by Société Générale.

5. Communication of personal data to third parties

Personal data processed by Société Générale may be communicated to the following recipients:

- employees, agents, representatives and consultants of Société Générale;
- other legal entities within the Société Générale Group;
- external legal advisors;
- external fraud detection services; and
- external service providers having a contractual relationship with Société Générale;

for the purpose of (i) managing its banking relationship, managing products and services, executing the account holder's orders and transactions, managing accounting procedures of the Group, notably when pooling resources and services with the Société Générale group and (ii) entrusting certain operational functions to other entities of the Société Générale Group or to service providers chosen for their expertise and reliability to provide specific services.

In such cases, Société Générale will take all physical, technical and organizational measures necessary to ensure the security and confidentiality of personal data.

Furthermore, Société Générale may also disclose personal data, upon request, to the official organs and administrative or judicial authorities of a country, located within or outside the European Economic Area, particularly in the context of the fight against money laundering and terrorist financing.

6. Transfer outside of the European Economic Area

Given the international scope of Société Générale group, and in order to optimize quality of services, the processing of personal data mentioned above may involve the transfer of personal data to countries outside the European Economic Area (EEA), whose legislation on the protection of personal data is different from that of the European Union.

The personal data may also be processed by staff operating outside of the EEA who work for our affiliates or other companies of Société Générale Group or for one of our suppliers and service providers.

Where we transfer personal data outside the EEA, we will ensure that it is protected in a manner that is consistent with how personal data will be protected by us in the EEA. This can be done in a number of ways, for instance:

- the third country that we send the data may be declared as offering an adequate level of protection through a European Commission decision ;
- where the recipient is located in the US, based on the EU-US Data Privacy Framework if the recipient of the personal data is certified ; or
- the recipient might have signed up to a contract based on "model contractual clauses" approved by the European Commission, obliging them to protect your personal data.

In other circumstances the law may permit us to otherwise transfer personal data outside the EEA. In all cases, we will ensure that any transfer of personal data is compliant with applicable data protection law.

More details of the protection given to personal data when it is transferred outside the EEA (including a copy of the standard data protection clauses which we have entered into with recipients of your personal data) can be obtained by contacting us in accordance with the "Contacting us" section below.

7. Retention of personal data

Personal data will be kept no longer than necessary in relation to the purposes for which they were collected or otherwise processed.

How long we hold your personal data for will vary. The retention period will be determined by various criteria including:

- the purpose for which we are using it – we will only keep the data for as long as it is necessary to achieve the purpose for which they are processed;
- legal obligations – laws or regulation may set a minimum period for which we have to keep your personal data; or
- the statutory limitation period for potential or existing claims.

Please consult the Annex to this Privacy Policy for a detailed overview of the retention periods of personal data processed by Société Générale.

8. Rights of the Data Subjects

The employees and representatives of the Clients (Data Subjects) have the following rights:

- the right to obtain information regarding the processing of their personal data and access to the personal data which Société Générale holds about them;
- in some circumstances, the right to receive some personal data in a structured, commonly used and machine-readable format and/or request that Société Générale transmits those data to a third party where this is technically feasible. This right only applies to personal data which the Data Subjects have provided to us;
- the right to request that Société Générale rectifies their personal data if it is inaccurate or incomplete;
- the right to oppose against the processing of their personal data for direct marketing purposes;
- where the processing is based on consent, the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them which is based on our legitimate interest, including profiling based on that legal ground. Société Générale shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subjects or for the establishment, exercise or defence of legal claims;
- the right to request that Société Générale erases their personal data in certain circumstances. There may be circumstances where the Data Subjects asks us to erase their personal data but we are legally entitled to retain it;
- the right to request that Société Générale restricts its processing of their personal data in certain circumstances. Again, there may be circumstances where the Data Subjects asks us to restrict its processing of their personal data but we are legally entitled to refuse that request.

Data Subjects can exercise their rights by contacting us using the details set out in the “Contacting us” section below, including a copy of both sides of the ID cards of the relevant individuals.

Société Générale will carry out requests promptly unless we will have a strict business interest not to fulfill requests to the extent permitted by law. Société Générale will revert on how requests will be handled within 1 month after reception of the request.

Data Subjects may also lodge a complaint with the local data protection authority if they deem it appropriate.

For the Netherlands, the competent data protection authority is the “Autoriteit Persoonsgegevens”, Postbus 93374, 2509 AJ Den Haag. Further contact details can be found on the website of the Autoriteit Persoonsgegevens: <https://autoriteitpersoonsgegevens.nl/>.

9. Security of personal data

Société Générale takes all reasonable physical, technical and organizational measures needed to ensure the security and confidentiality of personal data, particularly in view of protecting it against loss, accidental destruction, alteration, and non-authorized access.

Société Générale applies strict security measures to protect the confidentiality and integrity of personal data when transferring, storing or processing it.

Société Générale uses physical, administrative and technical security measures to reduce the risk of loss, misuse or unauthorized access, disclosure or modification of personal data. All of Société Générale’s employees have signed a confidentiality agreement.

Société Générale stores personal data on secure servers that are located either at our offices, at the offices of our subcontractors, or at fully classed data centers. Only authorized personnel can access the information on these servers. Where our Clients’ personal data needs to be disclosed to our subcontractors, we require them to process and protect personal data in a manner consistent with this Privacy Policy and applicable laws.

10. Contacting us

In case of any questions or concerns about any information in this Privacy Policy or the exercise of the rights provided in this Privacy Policy, please contact:

Data controller contact details:

GDPR-BE@sgcib.com

Data Protection Officer:

GDPR-DPO-BE@sgcib.com

GLOSSARY OF TERMS

Personal data

Information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified directly or indirectly.

Data Controller

Entity which determines the purposes and means of a processing of personal data

Processing

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

Processor

Any person or entity which processes personal data on behalf and upon instructions of the data controller.

AGGREGATED PROCESSES

Process purpose	Detailed process purpose	Categories of personal data	Legal basis for processing	Data Retention
KYC/AML/Fraud prevention/criminal offences	The prevention and detection of fraud and related crimes, identification controls, checking transactions, operational risk management, prevention of conflicts of interests, producing statistics, management information and executing tests, complying with anti-money laundering, terrorism and related legislation and complying with other legal and regulatory obligations.	<p>Identification data (including personal contact details, image and nationality), professional life (including professional contact details), financial data (including bank details and banking operations), commercial & contractual data, operations & services, incident prevention and management</p> <p>For board members and main directors, categories of personal data above + family relationship when linked to their professional activities</p>	<p>Necessary for compliance with a legal obligation</p> <p>Legitimate interest</p>	<p>Personal data will be retained until the end of the Client 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 in accordance with our legal obligations</p>

Financial management	Own accounting, performance monitoring, solvency and treasury management Producing regulatory reports and financial communication	Identification data (including personal contact details, image and nationality), professional life (including professional contact details), technical data (including connection and authentication data)	Necessary for compliance with a legal obligation	Personal data will be retained until the end of the Client relationship and for an additional period of maximum 10 years in accordance with legal obligations relating to accounting and tax
Management of the business relationship	During this phase we collect and store what is necessary for product/services provisions	Name of operational contacts, professional phone numbers, professional address, job title, scope of delegation, professional e-mail	Processing necessary for compliance with a legal obligation Legitimate interest	Personal data will be retained until the end of the Client relationship and for an additional period of maximum 5 years, in accordance with legal obligations and taking into the account the statutory limitation period
Securities Services provision	While executing the contracts with our Clients, we often need to store and handle data in addition to the basic data collected during the on-boarding phase	Depending on the services, we collect personal data from final investors and holders: Identification data (including personal contact details, image and nationality), professional life (including professional contact details), technical data (including connection and authentication data), financial information	Necessary for the performance of a contract Legitimate interest	Personal data will be retained until the end of the Client relationship and for an additional period of maximum 5 years, 10 years, or 30 years in accordance with legal obligations and taking into the account the statutory limitation period

<p>Payment services Provision</p>	<p>While executing the contracts with our Clients, we often need to store and handle personal data in addition to the basic personal data collected during the on-boarding phase</p>	<p>Depending on the services, we collect personal data from final beneficiaries, including identification data, data related to bank details and banking operations, financial information, smart card or IBAN identifier</p>	<p>Necessary for the performance of a contract Legitimate interest</p>	<p>Personal data will be retained until the end of the Client relationship and for an additional period of maximum 5 or 10 years, in accordance with legal obligations and taking into the account the statutory limitation period</p>
<p>Capital markets services Provision</p>	<p>While executing the contracts with our Clients, we often need to store and handle personal data in addition to the basic personal data collected during the on-boarding phase</p>	<p>Depending on the services, we collect personal data from final investors and holders: identification data (including personal contact details, image and nationality), professional life (including professional contact details), technical data (including connection and authentication data), financial information</p>	<p>Necessary for the performance of a contract Legitimate interest</p>	<p>Personal data will be retained until the end of the Client relationship and for an additional period of maximum 5 or 10 years, in accordance with legal obligations and taking into the account the statutory limitation period</p>

Structured finance Products offer and delivery	While executing the contracts with our Clients, we often need to store and handle personal data on their representatives in addition to the basic ones collected during the on-boarding phase	In this context, we process personal data of our Clients' representatives: Identification data (including personal contact details, image and nationality), professional life (including professional contact details), technical data (including connection and authentication data)	Legitimate interest	Personal data will be retained until the end of the Client relationship and for an additional period of maximum 5 or 10 years, in accordance with legal obligations and taking into the account the statutory limitation period
Corporate Finance Services provision	While executing the contracts with our Clients, we often need to store and handle data in addition to the basic data collected during the on-boarding phase	Depending upon the services (Mergers and Acquisitions, Equity Capital Market, Corporate Brokerage), we: - collect personal data from issuers and investors: Identification data (including personal contact details, image and nationality), professional life (including professional contact details), technical data (including connection and authentication data), financial information -	Necessary for compliance with a legal obligation Necessary for the performance of a contract Legitimate interest	Personal data will be retained until the end of the Client relationship and for an additional period of maximum 10 years, in accordance with legal obligations and taking into the account the statutory limitation period

<p>Management of websites (relevant privacy policy and cookie policy will be available on each website)</p>	<p>Our open websites help a prospect, Client, candidate to better know our offers, locations and distribute our public communication</p>	<p>We use strictly necessary cookies to manage the content of our websites. We also use cookies for analytical purposes, for which we request your consent.</p>	<p>Consent (for the placing of cookies that are not strictly necessary for the functioning of the website)</p> <p>Our legitimate interest to enhance website security and improve user experience (for the placing of cookies that are strictly necessary)</p>	<p>Please consult the privacy policy and cookie policy on each website for the relevant retention periods</p> <p>https://www.societegenerale.nl/en/cookies-policy/</p> <p>https://global.societegenerale.com/en/gdpr/</p>
<p>Develop business with corporate prospects or existing counterparts and clients such as corporate/financial institutions</p>	<p>Marketing purposes (unless Clients tell us not to), organising commercial events, offering new services, and conducting statistical and private capital surveys (including behavioral surveys).</p>	<p>We process:</p> <ul style="list-style-type: none"> - clients/prospects' professional e-mail/ address and mobile phone. - Personal preferences for rooms in hotels or meals 	<p>Legitimate interest</p>	<p>Personal data used for marketing purposes will be retained until the end of the Client relationship or until the Client objects against this processing.</p> <p>Personal data used to invite Clients or prospects to events will be retained for a period of up to 1 year after the event, according to the agreements we have with the third parties</p>

Security of premises	We process personal data of visitors at our premises for security reasons	Names and company of visitor at the entrance desk	Legitimate interest	Personal data used to ensure security of premises will be retained for a maximum period of 7 years in accordance with legal obligations
----------------------	---	---	---------------------	---

Annex : list of legitimate interests

Where necessary and indicated in this Privacy Policy, Société Générale processes your personal data in order to safeguard the legitimate interests pursued by us or by a third party. Those legitimate interests are as follows:

1. **Fraud Prevention and Security:** Ensuring the security of the bank's systems and transactions to protect against misconduct, fraud and cyber-attacks, including the prevention of banking system failures, fraud, money laundering, terrorism financing, and cybercrime, along with compliance with international sanctions and embargoes. Measures for building and systems security (e. g. admittance and visitor control), to protect our property and to ensure against trespassing;
2. **Compliance with foreign Legal Obligations:** ensuring compliance with local regulations in the countries where Société Générale operates, including adherence to authorities' and regulators' requirements and recommendations, even outside Europe.
Business Operations, Service Improvement and customer experience: Enhancing and developing banking services, conducting market research, surveys and tests and improving operational efficiency.: Maintaining and managing relationships with corporate clients and their representatives, including organisation of events or promotional campaigns to promote our products and services communications regarding services, updates, and changes.
3. **Risk Management:** Assessing and managing financial risks, including credit risk, market risk, and operational risk.
4. **Marketing and Communications:** Sending relevant marketing communications to corporate clients about products and services that may be of interest, ensuring that such communications are conducted in a lawful and non-intrusive manner conducting market and opinion research.
5. **Defending rights and litigation:** asserting legal claims and mounting a defence in case of litigation
6. **Business management and product development:** Measures to manage business, further develop and improve services and products; Management of our products and services provided to clients, including where the processing of personal data of a person who is not party to a contract is required;
7. **Advertisement and market studies:** Advertising or market and opinion research, to the extent that Client has not objected to having their data used;
8. **Internal Reporting and Analytics:** Conducting internal audits, financial analysis, and reporting to improve business performance and decision-making.