

## GENERAL PRIVACY POLICY

### Data protection notice

The following is intended to provide you with information about the processing of your personal data and your rights under applicable data protection law, particularly having regard to the transparency requirements under Articles 12 to 14 GDPR and the information required to be communicated under Articles 15 to 22 and Article 34 GDPR about the rights of data subjects under the GDPR.

The general privacy policy is supplemented by the Cookie policy.

#### Data controller:

Societe Generale S.A., Zweigniederlassung Frankfurt  
Neue Mainzer Straße 46-50  
60311 Frankfurt am Main

Tel.: 0 69 / 71 74- 0

Fax: 0 69 / 71 74- 1 96

Email: [datenschutz@sgcib.com](mailto:datenschutz@sgcib.com)

#### Contact details of our Data Protection Officer:

Societe Generale S.A., Zweigniederlassung Frankfurt  
Data Protection Officer  
Neue Mainzer Straße 46-50  
60311 Frankfurt am Main

Tel: 0049 69 7174-484

Email: [datenschutzbeauftragter@sgcib.com](mailto:datenschutzbeauftragter@sgcib.com)

### A. Sources and data

We primarily process personal data received from legal representatives and employees of companies with whom we have or are initiating contact for business purposes (business contacts). To the extent necessary for the performance of our service, we also process personal data that we have lawfully received from our clients (e.g. in order to execute transactions, to perform contracts, to send fund reports), or based on your consent.

In addition, we process personal data that we receive in the course of our business relationship with our service providers. We also process personal data that we have lawfully obtained from publicly available sources (e.g. the commercial register) and which we are permitted to process.

The following may be relevant personal data in connection with our business relationship with you personally or in your capacity as a representative, employee, counterparty or shareholder of our clients:

Name, office address or other business contact details (telephone number, fax number, email address), residential address or other private contact details (telephone number, fax number, email address).

In addition to the data referred to above, other personal data from the following categories may be processed:

#### Business contact details

Other personal data arises in the course of initiating or negotiating business and during the business relationship, particularly as a result of face-to-face meetings, telephone calls or written correspondence, whether initiated by you or us. This data includes inter alia information about professional position held, name of the employer, place of work, the channel of communication, the date, (electronic) copies of correspondence and information about participation in direct marketing campaigns.

#### Account transactions and payments

Transaction data is recorded from payment orders as well as data from the performance of our contractual obligations (payment data).

#### General due diligence requirements

We collect details such as your surname, first, place of birth, data of birth, gender, family situation, nationality, personal data relating to criminal conviction or offences and residential address prior to establishing a business relationship in order to comply with anti-money laundering laws.

#### Information from end devices

Information from end devices: We also collect data that we have received from the devices you use (computer, tablet, mobile phone, etc.), such as IP addresses.

Furthermore, the following types of data will be collected and processed:

- Connection data related to the use of our online services: identification and authentication data for your connected spaces, logs, cookies, browsing data on Societe Generale sites and applications (SG Markets etc.)
- Data processed as part of the electronic signatures: inter alia, signatories' identification data, timestamp, logs.

### B. Purpose of data processing and the legal basis for such processing

We process the above personal data in accordance with all applicable German and European regulations relating to the protection of personal data, in particular the General Data Protection Regulation (EU) 2016/679, the German Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) and Telecommunications Digital Services Data Protection Act -TDDDG.

The corporate purpose of Societe Generale Frankfurt/Main comprises the following:

- Banking business of any kind as defined in section 1 of the German Banking Act (Kreditwesengesetz – KWG).
- Storing and processing personal data for own purposes and at the instruction and on behalf of group companies pursuant to the Group's service agreements.
- Uncovering, preventing or prosecuting money laundering, fraud and other crimes in accordance with our statutory obligations.

Personal data is used solely for the following specific purposes:

**a) in order to perform contractual obligations (point (b) of Article 6 (1) GDPR)**

Data is collected and processed within the scope of the aforementioned corporate purpose for the purposes of providing financial services in the course of performing our contracts with our clients, or in order to take steps at the data subject's request prior to entering into a contract.

**b) based on legal requirements (point (c) of Article 6 (1) GDPR) or in the public interest (point (e) of Article 6 (1) GDPR)**

As a bank, we are subject to various legal obligations, in other words statutory requirements under German legislation such as the Banking Act, the Investment Code (Kapitalanlagegesetzbuch), the Money Laundering Act (Geldwäschegesetz), the Securities Trading Act (Wertpapierhandelsgesetz), tax legislation, criminal procedure law, the Investment Tax Act (Investmentsteuergesetz) and prudential requirements (e.g. imposed by the European Central Bank, the Committee of European Banking Supervisors, the German Bundesbank, the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin) or the Autorité des marchés financiers (French financial markets regulator) and other European supervisory authorities). The purposes of processing include checking identity and good repute, preventing fraud and money laundering, combating terrorist financing, complying with verification and notification requirements under tax law and checking investment rules, assessing and managing company risks, ensuring the security and operation of IT systems and taking steps to ensure the security of buildings and equipment (e.g. access controls).

**c) in order to balance interests (points (f) and (d) of Article 6 (1) GDPR)**

Where necessary, we also process data to protect our legitimate interests or those of third parties. Our legitimate interests are as follows:

- Performing contracts with our clients or taking steps prior to entering into a contract (if the data subject is not the client)
- Establishing legal claims and defending legal actions
- Ensuring the security of infrastructures and transactions and operation of the Bank's IT systems, prevent the risks of banking systems failure
- Signature verification (through documents for checking authentication or through extracts from the commercial register)

- Preventing fraud, fight against money laundering, terrorism financing and cybercrime, compliance with regulation relating to international sanctions and embargoes and investigating criminal offences (if not already covered by b)
- Ensuring compliance with local regulations to which Societe Generale Group is subject given its activities and/or in the countries where Societe Generale is established to meet the requirements and recommendations of authorities and regulators, including countries outside the European Union
- Assessing and managing financial risks, including credit risk, market risks and operational risks, and ensuring the effectiveness of internal controls
- Taking steps to ensure the security of buildings and equipment (e.g. access controls)
- Taking steps to ensure compliance with building rules (e.g. video surveillance)

**d) based on your consent (point (a) of Article 6 (1) GDPR or, if applicable, in accordance with Section 25 (1) Telecommunications Digital Services Data Protection Act - TDDDG)**

Where you have given us your consent to the processing of your personal data for specific purposes, we will process your data on the basis of and in accordance with that consent. You will be informed separately in advance about the details of the data processing. You may withdraw your consent at any time with effect for the future; any such withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

## C. Recipients of the personal data

Within our bank, access to personal data is only given to functions and departments that need it in order to fulfil our contractual and statutory obligations. For this purpose we also make use of internal and external service providers or subcontractors who process data on our behalf, and they may also receive the data.

With regard to the disclosure of data to recipients outside our company, we would firstly like to point out that we are bound by a duty to keep all personal details and ratings/assessments of which we become aware strictly confidential. We are only permitted to disclose information about you if required to do so by law, if you have given your consent, if we are authorised to provide information and/or service providers commissioned to process data on our behalf similarly guarantee to comply with the duty to ensure banking secrecy and the requirements of the GDPR/the BDSG.

Subject to these requirements, the following categories of recipient may receive personal data:

- Where a statutory or regulatory requirement exists, public sector agencies and institutions (e.g. BaFin, the European Securities and Markets Authority (ESMA), tax authorities, the Federal Central Tax Office

(Bundeszentralamt für Steuern), the Autorité des marchés financiers (AMF), European supervisory authorities or investigating authorities).

- Other member entities of our Group, advisers, lawyers, auditors, institutional investors, depositories, brokers, similar institutions and group companies and service providers processing data on our behalf to which we send personal data for the purpose of carrying on our business relationship with you or with our clients. This may specifically involve: archiving, debt collection, document processing, call center services, compliance services, controlling, data screening for anti-money laundering purposes, data destruction, support/maintenance of IT applications, funds management, purchasing/procurement, space management, client management, group services, marketing, reporting, risk control, expense accounting, securities services, auditing services, payments.

Other data recipients may include functions or departments for which you have given your consent to the transfer of data.

#### **D. Data transfer outside the European Economic Area**

Data is transferred to agencies in countries outside the European Union (EU) or the European Economic Area (EEA) ("third countries") where required by law, where you have given us your consent, or where it is authorised under data protection law based on the existence of legitimate interests and does not conflict with any compelling legitimate interests on the part of the data subject.

Where the recipients of your data, particularly our service providers or their subcontractors, have their registered office outside the EU/EEA, it may be that the applicable laws ensure a different level of data protection in that country compared to the level prescribed under European data protection law. Where this is the case, we ensure (e.g. by entering into appropriate contracts (Article 46 (2) GDPR)) that the service provider concerned guarantees an appropriate level of data protection comparable to the level of protection in Germany, e.g. by signing the Standard Contractual Clauses established by the European Commission. In addition, appropriate and additional security measures may be put in place to ensure the level of protection of personal data transferred outside the EEA.

Additional written agreements are not required in the case of third countries which the European Commission has decided ensure an appropriate level of protection for personal data in Europe (Article 45 GDPR). A copy of the relevant suitable and adequate safeguards is available from our Data Protection Officer. Beyond this, we do not transfer any personal data to international organizations.

#### **E. Duration of data storage**

We process and store your personal data for as long as is necessary for the purpose for which it is processed and necessary in order to fulfil our contractual and statutory obligations.

Where the data is no longer necessary for the purpose for which it was processed or to fulfil contractual or statutory obligations, it is erased or rendered anonymous, unless it is necessary to store (for a fixed term) or continue to process the data for the following purposes:

- To comply with commercial or tax law retention periods: Relevant legislation here includes the German Commercial Code (Handelsgesetzbuch), the German Fiscal Code (Abgabenordnung), the Money Laundering Act and the Securities Trading Act, as well as other regulatory provisions. The retention or record keeping periods prescribed in those statutes are between two and ten years.
- To preserve evidence in accordance with provisions relating to the limitation of actions. Pursuant to sections 195 et seq. of the German Civil Code (Bürgerliches Gesetzbuch – BGB), limitations periods can be up to 30 years, although the usual limitations period according to the civil code is three years.

#### **F. Obligation to provide data**

As a governing body or employee of our clients, in the course of the business relationship you are required to provide the personal data necessary for commencing and carrying on the business relationship and for fulfilling the associated contractual obligations to our clients, or the personal data we have a legal obligation to collect. Without this data, we will usually have to decline entering into a contract or executing a transaction or will no longer be able to perform an existing contract and may have to terminate it.

In particular, we are required under anti-money laundering laws to verify your identity before a business relationship is established with our clients, for example by checking your personal identification card, and in so doing we are required to record your name, place of birth, date of birth, nationality and your residential address. In order for us to be able to comply with this statutory obligation, you are required under the Money Laundering Act to provide the necessary information and documents and to notify us without undue delay of any changes arising in the course of the business relationship. If you fail to provide us with the necessary information and documents, we may decline to enter into or continue the desired business relationship with clients.

## G. The security of personal data

Societe Generale takes all physical, technical and organizational measures to ensure the confidentiality, integrity and availability of personal data, in particular to protect the personal data 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, Societe Generale will notify the breach to the Data Protection Officer of Hesse ([datenschutz.hessen.de](https://datenschutz.hessen.de)) in compliance with the regulatory deadline. If this personal data breach presents a high risk to the rights and freedoms of natural persons, Societe Generale will inform you as soon as possible of the nature of this breach and the remedial action taken.

## H. Your data protection rights

Each data subject generally has the following rights:

- Right of access (Article 15 GDPR). You have the right to obtain confirmation from us as to whether or not your personal data is being processed. Where that is the case, you have the right to certain information and the personal data. The right of access particularly includes access to information regarding the purposes of processing, the categories of personal data concerned, and the recipients or categories of recipient to whom the personal data has been or will be disclosed. Please note that this right of access is not an absolute right and may be restricted by the legitimate interests of others. The right of access may be limited by section 34 of the Federal Data Protection Act.
- Right to rectification (Article 16 GDPR). You have the right to have inaccurate personal data concerning you rectified. Taking into account the purposes of the processing, you also have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
- Right to erasure ("right to be forgotten") (Article 17 GDPR). Where the relevant prerequisites are met, you have the right to have your personal data erased without undue delay. The right to erasure may be limited by section 35 of the Federal Data Protection Act.
- Right to restriction of processing (Article 18 GDPR). Where the relevant prerequisites are met, you have the right to have the processing of your personal data restricted. Where this is the case, the personal data will be identified accordingly and, if applicable, only processed for certain purposes.
- Right to data portability (Article 20 GDPR). Where the relevant prerequisites are met, you have the right to the data portability of the personal data you provided to us, in other words you have the right to receive that data in a structured, commonly used and machine-readable format and, if applicable, the right to transmit that data to another controller without hindrance from the controller to which the personal data was provided.
- You also have the right to lodge a complaint with a competent supervisory authority (Article 77 GDPR in conjunction with section 19 BDSG).

You have the right to inform us at any time that you withdraw your consent to the processing of your personal data. The withdrawal of consent shall not affect the lawfulness of processing up until such withdrawal. The withdrawal of consent has prospective effect only. The processing of data prior to the withdrawal is not affected.

## I. Automated decision-making

We basically do not make use of any fully automated decision-making as referred to in Article 22 GDPR to establish and carry on business relationships. Should we implement automated decision-making in individual cases, we will notify you separately.

## K. Profiling

Due to legal and regulatory requirements, we are obliged to take precautions against money laundering, terrorist financing and criminal offences. Screening of data (e.g. in payment transactions) are also carried out. These measures have been also implemented to protect our clients and partners. In addition, no automated data processing is carried out, in particular no tracking tools or cookies are used for this website.

### Right to object under Article 21 GDPR

You have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data based on legitimate interests (point (f) of Article 6 (1) GDPR). This also applies to any profiling within the meaning of Article 4 (4) GDPR based on this provision. We will no longer process your personal data unless we are able to demonstrate compelling legitimate grounds for such processing which override your interests, rights and freedoms, or the processing is in the interests of the establishment, exercise or defence of legal claims.

You also have the right to object to the processing of your personal data for direct marketing purposes without charge and without giving reasons. The same applies with respect to the processing of your personal data, including profiling to the extent it is related to such direct marketing. We will thereafter no longer use your data for these purposes (Article 21 (2) GDPR).

### Addressee for objections

There is no prescribed form for objections. Please include "objection" in the reference/subject line, provide your name and address, and send to:

Societe Generale S.A., Zweigniederlassung Frankfurt  
Neue Mainzer Straße 46-50  
60311 Frankfurt am Main

or send by email to: [datenschutz@sgcib.com](mailto:datenschutz@sgcib.com)