Data Protection Information in accordance with Articles 13, 14 GDPR for Clients (B2C)

(01.01.2026)

With the following information, we would like to inform you about the processing of your personal data and provide you with an overview of your rights under the EU General Data Protection Regulation (GDPR). Please note that not all components of this letter apply to you, as the question of which data is processed in detail and how it is used depends significantly on the agreed services.

I. Data Controller and Data Protection Officer

The Data Controller is
FIB Frankfurt International Bank AG (hereinafter "FIB AG")
Wilhelm-Leuschner-Straße 27-29
60329 Frankfurt am Main
Germany
Tel.: +49 69 - 247433980
Email: info@fib-ag.com
Website: https:www.fib-ag.com
You can reach our Data Protection Officer of AGOR AG at: info@agor-ag.com or by phone: +49 (0) 69 - 9494 32 410. The contact details are also available on the internet at www.agor-ag.com .
In addition, you have the option to use the email address for data protection concerns datenschutz@fib-ag.com .

II. Categories of Data, Legal Basis and Purposes of Processing

1. Processed data categories

We collect your personal data when you contact us, for example, as a prospective or actual client.
In particular, if you are interested in our products or services, contact us by email or telephone, or use our products and services within the framework of existing business relationships.
We also process personal data from publicly accessible sources if this is necessary for our service.
We lawfully obtain this data, for example, from land registers, debtor directories, or commercial and association registers. Personal data is also transmitted to us by other third parties (e.g., credit agencies). We also use directories of certain individuals within the scope of legally mandated checks for money laundering prevention.
The following personal data we process, provided we have collected them for the establishment of a business relationship and the fulfilment of contractual relationships:

- Personal Identification Information
  e.g. First and last names, address, if applicable Date of birth and place of birth, gender, nationality, identity card/passport number, email address, telephone number, tax identification number, if applicable. Authentication data (e.g., signature specimen)

- Order and sales data

  e.g. IBAN, payment orders (incoming and outgoing payments), data from the fulfilment of our contractual obligations

(e.g. payment transaction data)

- Data about your financial situation

  e.g. payment behaviour, value of other assets, entries in credit agencies, payment default, third-party data, quality data, tax information, details on any third-party beneficiaries, documentation data (e.g. consultation records/offer), direct debit data, (credit) contracts, creditworthiness documents, scoring/rating data, information/evidence on the purpose of use, own and third-party securities.

- Information about your interests and preferences that you provide to us

  e.g. by letter, telephone or email contact including (electronic) copies of correspondence and, if applicable, information about participation in direct marketing activities

- audiovisual data, e.g. information from video conferences or possibly the video identification procedures.

In the case of personal guarantees by third parties (external securities), we may impose comparable requirements on the respective guarantor for the disclosure of economic and financial circumstances.
As well as other data comparable to these categories.
Special categories of personal data (within the meaning of Art. 9 GDPR), known as "Sensitive Data," such as information regarding your political or religious affiliation, are only collected by us when it is absolutely necessary. For example, for PEP screening under the Money Laundering Act and matching with sanctions lists.
If you select a video identification process through certain service providers, such as WebID (link to their privacy policy https://webid-solutions.com/de/datenschutz/), biometric data will also be processed, which fall under the category of special personal data within the meaning of Art. 9 GDPR. The legal basis for the processing is the consent you are to grant, which you can revoke at any time in accordance with Section IV.
We only collect information about persons under 18 years of age if you open an account for minors.

2. Contractual Relationship between Company and Client (B2C)

As part of our contractual relationship with our private clients, we process data within the master data management. This generally includes the management of data within our CRM system (or core banking system Finastra, of Finastra International GmbH, located at Hedderichstraße 36, 60594 Frankfurt), document management (e.g. Fintiba GmbH, Wilhelm-Leuschner-Str. 29, 60329 Frankfurt am Main) and storage, the use of cloud services (e.g. Microsoft 365 of Microsoft Ireland Operations Limited, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland), and the creation of system-side logs. Within internal communication and external communication with our private clients, we utilise the usual communication channels, which take place particularly via email, telephone, and in writing (by post). In addition, private client management includes, among other things, the creation of presentations/tables, the exchange of documents, as well as chat communication and participation in audio and video conferences via cloud services.
You have the opportunity to notify us of data changes (e.g. new mailing address, new contact persons, changed Bank details) or other concerns related to an existing contractual relationship (e.g. complaints, termination) through the corresponding channels on our website www.fib-ag.com or via info@fib-ag.com (including online). For this purpose, you may also need to provide address, contact, and communication data, as well as, if applicable, information about your contractual relationship with us, so that we can process your request. Furthermore, we refer to the possibility of exercising your rights as a data subject concerning data processing under Chapter IV of this Privacy Policy.

The legal basis for data processing and communication with persons with whom we have a business relationship is, in accordance

with Art. 6 para. 1 sentence 1 lit. f GDPR, our legitimate interest, which consists of being able to manage the contractual relationship with the persons with whom we have a contractual relationship.
We disclose your data for specific purposes and in compliance with data protection regulations to the sales, marketing, and service providers commissioned by us, who support us both in fulfilling the contract and in communication with our private clients. We contractually require them under the GDPR not to use your data for their own purposes or to disclose it to other third parties.
We delete the personal data as soon as it is no longer required for the above purposes. After the termination of the contractual relationship, the personal data will be stored as long as the responsible entity is legally required to do so. The statutory retention periods (e.g., in accordance with the German Commercial Code, Fiscal Code) generally amount to up to ten years.
In addition, we process your data in individual cases for statistical evaluations and for the further development of our services and products.

a) Setting up an account for private clients

In order to fulfil our contracts, we must process your data. This also applies to pre-contractual measures and information you provide to us in the context of contacting us or submitting an application. The purposes of data processing are primarily determined by the respective product (e.g. current account or blocked account) and may include, among other things, needs analyses, advisory services, and the execution of transactions. The further details regarding the purpose of data processing can be found in the respective contract documents and terms and conditions.
The legal basis for processing your data within the framework of the contractual relationship with you is Art. 6 para. 1 sentence 1 lit. b GDPR.
For instance, we receive order data for the processing of payment services and transmit payment data as instructed to payers, payees, and their banks.
We also require your personal data to be able to check whether we can and are allowed to offer you a product or service.
For the execution of our contractual relationship, an online user account is also required, which is created through a one-time registration. You can find further information on this in the privacy policy on our website www.fib-ag.com.

Encrypted payment transactions
If, after concluding a contract that involves a charge, you are required to provide us with your payment details (e.g., account number for direct debit authorization), this data is required for payment processing.

Payment transactions using common payment methods (Visa/MasterCard, direct debit) are carried out exclusively via an encrypted SSL or TLS connection. You can recognize an encrypted connection by the fact that the address line of the browser changes from “http://” to “https://” and by the lock symbol in your browser line.
With encrypted communication, your payment details that you transmit to us cannot be read by third parties.

b) Payment processing

In General

Essential for the fulfilment of the contract are payment transactions within our contractual relationship. For this purpose, external payment service providers are used.
We, or the payment service providers engaged, collect and process necessary inventory data for the transaction, such as contact details, Bank data/credit card numbers, passwords, and contract information. The collected data will be processed and stored solely by us or the selected service provider. Individual payment service providers may, under certain circumstances, transmit your personal data to credit agencies for the purpose of a credit check.
The legal basis for processing is our contractual relationship in accordance with Art. 6 para. 1 sentence 1 lit. b GDPR.

Google Pay

When paying via Google Pay, we pass on your payment details to Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland (hereinafter "Google Pay") for the purpose of payment processing.

The transfer is carried out in accordance with Art. 6 (1) (b) GDPR and only to the extent necessary for payment processing. Google Pay Corp. (GPC) may transfer, process, and store personal data outside the EU. Furthermore, the data collected by Google, including information obtained from third-party providers, is also made available to Google's subsidiaries.

You can object to this processing of your data at any time by sending a message to Google.

In addition, you have the option of objecting to the exchange of information about your creditworthiness between Google Pay Corp. and its affiliated subsidiaries. You can also object to the use of your data for advertising purposes. To do so, visit the Google Payments privacy settings page at https://accounts.google.com/v3/signin/identifier?dsh=S-1123292812%3A1672312333702563&continue=https%3A%2F%2Fpayments.google.com%2Fpayments%2Fhome%3Fpage%25253DprivacySettings%252523privacySettings%3A%23&followup=https%3A%2F%2Fpayments.google.com%2Fpayments%2Fhome%3Fpage%25253DprivacySettings%252523privacySettings%3A&osid=1&passive=1209600&service=billing&flowName=GlifWebSignIn&flowEntry=ServiceLogin&ifkv=AeAAQh5IVQIKmsmgj5QvIGNgNo8t36lmLxcQmWBOzA00wlq9HtrR4Bb03MiH1pGxIYD37DqDAnNubQ and make the appropriate changes to your settings.

In doing so, Google Pay undertakes to provide appropriate safeguards in accordance with Art. 46 GDPR in the form of standard contractual clauses (see https://business.safety.google/adscontrollerterms/).

For more information on Google's data protection policy, please visit https://policies.google.com/privacy.

Payment processing – Apple Pay

When paying via Apple Pay, we pass on your payment details to Apple Inc, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland, for payment processing. Payment is made via your iOS, watchOS, or macOS device. You must authorize the payment by entering a selected code or by verification via "Face ID" or "Touch ID." The respective payment method you have stored will then be charged. Payment processing and the corresponding payment data are transmitted in encrypted form. Apple also uses additional security features to protect your payment. Apple does not store credit, debit, or prepaid card numbers at any time and does not have access to them.

The transfer is carried out in accordance with Art. 6 (1) (b) GDPR and only to the extent necessary for payment processing.

For information about Apple Pay and data protection, open "Settings" on your iOS device, then "Wallet & Apple Pay" and then "How your data is managed." Alternatively, you can also access this information on your Mac device. Go to System Preferences, then Wallet & Apple Pay, and then click Apple Pay & Privacy.

For more information about privacy with Apple Pay, visit https://www.apple.com/legal/privacy/data/

c) Processing to fulfil legal requirements

As a Bank, we are subject to numerous legal requirements (e.g. from the Money Laundering Act, the Banking Act, or the tax laws). We must also meet banking supervisory requirements (e.g., from institutions such as the Federal Financial Supervisory Authority (BaFin), the Deutsche Bundesbank, the European Central Bank, or the European Banking Authority).

The processing of data serves, among other things, the following purpose: The creditworthiness check, the identity and, if applicable, Age verification, compliance with tax and banking supervisory control and reporting obligations, fraud and money laundering prevention, as well as risk assessment and management.

f) Processing within the scope of a balancing of interests

To the extent necessary, we process your data beyond the actual performance of the contract to safeguard legitimate interests of

ours or those of third parties.

- Consultation and data exchange with credit agencies to determine creditworthiness or default risks,
- Examination and optimisation of procedures for needs analysis and direct client approach; including client segmentation and calculation of closing probabilities,
- Advertising or market and opinion research, provided you have not objected to the use of your data,
- Assertion of legal claims and defence in legal disputes,
- Guarantee of IT security and IT operations,
- Prevention of crimes,
- Measures for business management and the further development of services and products,
- Risk management
- For the processing and response to complaints, if the complaint concerns another contracting party of the client, such as FIB AG in the case of investments with partner banks.

3. Complaint management

You have the opportunity to inform us of complaints at any time. For this, in addition to the email address info@fib-ag.com, our general telephone number is also available.
To process your complaint, the following personal data may be collected:

- Names
- Address
- Telephone number
- Email address
- Your message
- Possibly further data necessary for processing your complaint

The legal basis for this is generally the fulfilment of the contract within our client relationship in accordance with Article 6(1)(1)(b) GDPR.

Should you not have a direct contractual relationship with us, we process your data within the framework of communication based on our legitimate interest in accordance with Art. 6 para. 1 sentence 1 lit. f GDPR, which consists of being able to diligently and reliably handle any inquiries we receive.
We use the collected data solely for the processing and response to your complaint. No transfer of the data to third parties takes place. However, in order to process your complaint, it may be necessary to pass it on to internal company departments. The data will be deleted once the processing of the complaint is completed, provided that no legal obligations oppose this.

4. Visitor

If you visit our premises, we collect personal data for the purpose of access control, i.e., to control physical access. Further information on how we process your data in this context will be provided directly during your visit.

III. Further recipients of your data

In addition to the recipients already specified, those departments within FIB AG will have access to your data that need it to fulfil our contractual and legal obligations.

Furthermore, we may transfer your personal data to additional recipients outside the company, insofar as this is necessary to fulfil contractual and legal obligations. These can be, for example:

- Internal Audit
- Authorities (e.g. tax authorities, courts)
- Public authorities and institutions in the presence of a legal or official obligation
- Credit institutions for the processing of payment transactions
- Law firms and competent jurisdiction for the enforcement of claims
- Auditor for the execution of the statutory audit mandate
- Tax advisor

Further data recipients may be those entities for which you have granted us your consent to transfer data, or for which you have released us from the confidentiality obligation according to agreement or consent, or to which we are authorised to transfer personal data based on a balancing of interests.
Under no circumstances do we sell your data to third parties.

IV. Rights as a Data Subject

The data subject has the right to obtain from the Data Controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and information, as well as the right to rectification, erasure, restriction of processing, the right to object to processing, and the right to data portability.
If the data subject has given consent for further data use, they have the right to withdraw their consent at any time without stating reasons, with effect for the future.
The above rights can be asserted at:

FIB Frankfurt International Bank AG
Wilhelm-Leuschner-Straße 27
60329 Frankfurt am Main
Germany
Tel.: +49 69 - 247433980
Email: dataprotection@fib-ag.com
Notwithstanding the above rights, the data subject also has the option to contact the respective competent supervisory authority if they believe that the processing of their data violates the GDPR.

V. Retention period

Companies in Germany are subject to numerous statutory retention obligations, particularly from the Fiscal Code of Germany (AO) and the German Commercial Code (HGB). These laws provide for retention periods, e.g., for invoices, offers, or other contract-relevant documents, of up to ten years. Accordingly, we store your data, which we have collected in the course of pre-contractual measures or contract fulfilment, in accordance with the statutory retention periods. If the data are no longer required for the fulfilment of the purpose and there are no statutory retention obligations, the data will be deleted.
Provided you have given us your voluntary consent for data processing, we will store the data until your consent is revoked. A revocation is possible at any time for the future. Provided that no other purposes or retention periods oppose the deletion, your personal data will be deleted upon withdrawal of consent. Excluded from this are your first and last names, which are stored for three years in accordance with statutory evidence requirements. After the expiry of the statutory retention periods, your complete personal data (first name and surname) will be deleted.

Should separate deletion periods apply to the processing of your personal data in individual cases, you will find this information in each case under data processing in section II.

VI. Transfer to a third country

Depending on the specific service with an international connection that we provide for you, there is occasionally a transfer of your personal data to a third country. If this is the case, the transmission is based on appropriate safeguards in accordance with Art. 46 GDPR.

Furthermore, individual personal data is processed by FIB AG in the USA. Within the scope of the so-called "Data Privacy Framework" (DPF), the EU Commission also recognized the level of data protection as safe for certain companies from the USA under the adequacy decision of 10 July 2023. The list of certified companies as well as additional information regarding the DPF can be found on the website of the US Department of Commerce at https:www.dataprivacyframework.gov/s/participant-search . Furthermore, certain personal data are processed by FIB AG in the UK. The European Commission issued an adequacy decision for the United Kingdom on 28 June 2021, such that the UK is now considered a secure third country. Thus, the transmission of personal data after Brexit remains compliant with data protection regulations.

Furthermore, certain personal data are processed by FIB AG in Switzerland. On 15 January 2024, the European Commission confirmed the adequacy decision for Switzerland dated 26 July 2000, thereby recognising it as a safe third country. Thus, the transfer of personal data to Switzerland is possible in compliance with data protection regulations.

. Provision of the data

Within the scope of our business relationship, you must provide the personal data that is necessary for the commencement, execution and termination of a business relationship and for fulfilling the associated contractual obligations, or which we are legally required to collect. We point out that without the availability of this data, we will generally not be able to conclude, execute, and terminate a contract with you.

I. Automated individual decision-making and profiling

No automated individual decision-making or profiling measures take place.