Data Processing Information

Articles 13 and 14
General Data Protection Regulation (GDPR)

Dear customer !

Your trust in our institution is our greatest asset. We use utmost diligence and comply with the regulatory requirements when collecting and managing your personal data in the course of providing our services.

The following information for customers in accordance with Articles 13 and 14 of the EU General Data Protection Regulation (GDPR) describes how we process your personal data and the data privacy claims and rights available to you.

The nature and extent of data processing depends primarily on the products and services requested by you or agreed upon with you. This data privacy policy applies to the website **www.kathrein.at** of Kathrein Privatbank Aktiengesellschaft, 1010 Vienna, Wipplingerstraße 25.

Who is the data controller and whom can you contact?

Data Controller:
Kathrein Privatbank Aktiengesellschaft
Wipplingerstraße 25, 1010 Wien
E-Mail: datenschutz@kathrein.at

The Data Protection Officer of the bank:
Datenschutzbeauftragter:
Raiffeisen Bank International AG (RBI)
Am Stadtpark 9, 1030 Wien
E-Mail: datenschutzbeauftragter@rbinternational.com
Telephone: +43-1-71707-8603

What data do we process and from what sources?

We process the personal data we receive from you in the course of our business dealings with you. In addition, we process data we obtain legitimately from the record of debtors (Credit Protection Association 1870) and from publicly accessible sources (e.g. company register, association register, land register or media) or which are transmitted to us by other affiliates of the bank for legitimate interests.

The personal data comprise your personally identifiable data and contact data (e.g. name, address, date and place of birth, nationality etc.) or data relating to identity papers and travel documents (e.g. specimen signature, identification card data). It can also include payment transaction and clearing data (e.g. payment instructions, turnover data in payment transactions), creditworthiness information (e.g. type and amount of income, recurring payment obligations for schooling and education of children, loan payments, rent payments), data relating to marketing and sales, loan transactions, video and/or audio recordings (e.g. video or phone

recordings), electronic protocol and identification data (apps, cookies, IP addresses etc.), financial identification data (data relating to credit or debit cards) or AML (Anti Money Laundering) and compliance data, as well as other data similar in nature to the categories listed above.

What is the purpose and the legal basis for data processing?

We process your personal data in accordance with the provisions of the European Union General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

- **To fulfill contractual obligations [Art. 6 (1)(b) GDPR]**

Processing of personal data (Art. 4 (2) GDPR) occurs to provide and arrange for bank transactions and financial services including but not limited to performance under our agreements with you and execution of your orders as well as performance of pre-contractual measures.

The purposes of processing data is determined first and foremost by the specific product (e.g. account, loan, securities, deposits) and may, among other things, include needs assessments, consultation, asset management and administration and execution of transactions.

Such data processing occurs for example in connection with debit cards (also called ATM cards) provided to you by Kathrein and which you can use to execute payment transactions with retailers at POS terminals and online (e-commerce payments in online shops), to withdraw cash from respective ATM or cash machines and to facilitate transactions between debit cards ("ZOIN"). For those transactions, the financial institution of the card holder and of the recipient of the payment must be identifiable in order for those institutions to settle the transactions with each other. For that purpose, nearly all financial institutions operating within Austria have signed an agreement with PSA Payment Services Austria GmbH (PSA) (the PSA agreement). The agreement aims to regulate the mutual rights and obligations of the financial institutions and the PSA. The agreement stipulates the terms financial institutions have agreed upon regarding transactions (e.g. withdrawal of funds) executed by non-customers of the bank at bank-owned cash machines or payment transactions through POS terminals. PSA is responsible for the technical aspects of the transaction with eligible cards among those institutions. In addition, PSA operates its own ATMs or cash machines. To facilitate the transaction and settle payments between the financial institutions, the institutions must process the data of their own customers. The legal basis for processing data are a variety of Acts, e.g. the Austrian Banking Act (Bankwesengesetz), the Austrian Payment Services Act (Zahlungsdienstgesetz, ZaDiG), the Financial Markets Anti-Money Laundering Act (Finanzmarkt-Geldwäschegesetz, FM-GwG), etc., with which the parties to the PSA agreement must comply, and the agreement between the financial institution and its customer (e.g. checking account agreement, credit or debit card agreement). To exercise your rights in connection with the data processing measures listed above, please contact Kathrein.

For specific details regarding data processing activities referenced above, please read the respective agreements and relevant terms and conditions.

- **To fulfill legal obligation [Art. 6 (1)(c) GDPR]**

Processing of personal data might be necessary to fulfill a range of legal requirements (arising from the Banking Act, the Financial Markets Anti-Money Laundering Act, the Securities Supervision Act, the Stock Exchange Act etc.) as well as due to regulatory requirements (e.g. those established by the European Central Bank, the European Financial Authority, the Austrian Financial Market Authority etc.), which the bank is subject to as an Austrian financial institution. Examples are:

- Filing of suspicious activity reports with the Financial Intelligence Unit (Geldwäschemeldestelle) (Section 16 FM-GwG)
- Providing information to the FMA in accordance with the Securities Supervision Act (WAG) and the Stock Exchange Act (BörseG) in order to monitor compliance with the provisions governing the misuse of insider information in the market
- Providing information to the financial penalty authorities in response to financial penalty proceedings for deliberate financial crimes
- Providing information to federal tax authorities in accordance with Section 8 of the Austrian Accounts Register and Inspection of Accounts Act (Kontenregister- und Konteneinschaugesetz)
- Assessment and control of risks
- Credit check (credit scoring) for loan applications
  Credit scoring assesses the credit risk of the loan applicant by applying statistical comparisons of subpopulations. The resulting score is deemed to help assess the probability of repayment of a requested loan. To calculate the score, we use your master data (marital status, number of children, duration of employment, employer), information about your general financial status (income, assets, monthly expenses, collateral etc.) and information regarding your payment history (regular loan payments, payment reminders, data collected from credit agencies). If the risk of default is too high, the loan application will be denied.

- **As a result of your consent [Art. 6 (1)(a) GDPR]**

If you have given consent to processing of your personal data for certain purposes (e.g. transfer of data to the recipients named in the consent, notifications via ELBA, receipt of marketing material), the data will only be processed for the purposes and to the extent stated in the consent form. Consent can be withdrawn at any time and will become effective for future processing of data.

- **To safeguard legitimate interests [(Art. 6 (1)(f) GDPR] in general**

If necessary, for weighing the interests, data can be processed for the benefit of Kathrein and third parties to safeguard legitimate interests. In the following cases, data is processed to safeguard legitimate interests. Examples are:

- Inquiry with and exchange of data with credit agencies (e.g. Austrian Credit Protection Association 1870) to assess credit risk or risk of default
- Review and optimization of processes regarding needs analysis and direct communication with clients
- Video monitoring to collect data evidence in connection with criminal offenses or to furnish proof for orders and deposits (e.g. at the teller) – especially for the protection of customers and employees
- Certain telephone recordings (for quality assurance or in the case of complaints)
- Measures to controlling business and help develop services and products
- Measures for the protection of customers and employers as well as the property of the bank
- Measures to prevent and combat fraud (Fraud Transaction Monitoring), to combat money laundering, financing of terrorist activities and criminal offenses endangering assets. In this context, data will be analyzed (e.g. with payment transactions). Those measures are also for your own protection
- Processing of data for legal prosecution
- Assertion of legal claims and defense against legal disputes
- Ensuring IT security and IT operations within the bank
- Prevention and investigation of crimes

- **to safeguard legitimate interests [(Art. 6 (1)(f) GDPR] in marketing our services**

Analysis of your data processed by Kathrein in order to

- provide or send you customized information and offers of Kathrein and the companies named below, their products and services which Kathrein procures,
- develop services and products that match your interests and personal circumstances, as well as
- improve the ease of use of your service applications, such as TIPAS+, ELBA or other apps

is based on our legitimate interest in marketing our services. Processing of your data for this purpose continues as long as you do not object.

The following data collected by Kathrein or transmitted to Kathrein by you or at your request will be processed for that purpose:

- Personal Data/Master Data

Gender, professional title, name, date of birth, country of birth, nationality, marital status, tax status, level of education, profession, employer, authentication information such as driver's license data, income data, address and other contact data such as telephone number or email address, geographic location data, securities risk category in accordance with your investor profile, housing situation such as renter or owner and apartment or house, family relations (without collecting the personal data of those individuals), number of persons in the household, data provided during consultation sessions such as hobbies and interests or planned purchases and automobile, household expenses, internal ratings such as evaluation of income and expenses and assets and liabilities by Kathrein.

- Data regarding Kathrein products and

Data in connection with the Kathrein services utilized by you, including

- forms of payment used by you, such as credit and debit cards,
- debits and credits and outstanding payments on accounts and loans
- interest rates charged for those services, and charges and fees,
- payment history, including the options used by you to place orders (e.g. ELBA),
- incoming and outgoing wire transfers, payer and payee and providers transmitting payment orders, amount, description and payment references, client references,
- frequency and type of money transactions, with non-cash payments, the data of the merchants or service providers receiving payment and information about the transactions executed with them,
- data from ELBA,
- savings history and securities transactions and securities account balances, including details regarding securities held.

- Device and Contact Center Data (telephone hotline including interactive voice control)

Frequency, time and place of usage of contact centers (telephone service including interactive voice control) as well as audio and video recordings made in the course of using those services with reference to the relevant legal basis (e.g. in connection with support services for ELBA).

- Data from services, website and communications

Data for the use of electronic services and websites, use of features of websites and of apps and email messages between you and Kathrein, information regarding viewed web pages or content and links that were accessed, including external websites, information regarding the time it takes a user to react to content or download errors, the amount of time spent on a website as well as information on usage and about subscriptions of newsletters published by Kathrein.

This information is collected with the help of automated technologies such as cookies or web beacons (tracking pixel that registers access to emails or websites) or web tracking (tracking and analysis of search behavior) on the website or ELBA and with the help of external service providers or software.

Kathrein's website integrates the analytics tool of Digital Workroom. It does not use cookies or store personal data. When accessing a page, tracking pixels store country code, browser name and version, operating system, resolution and color scheme as well as the anonymized IP address in a unique key to be used for page statistics.

Kathrein does not use plugins or similar tools that transmits data to third party providers. Digital Workroom statistics analyzes user behavior without using personal data. Kathrein does not use social media plugins.

- Account and portfolio data accessed online

Data regarding information about accounts and portfolios accessed online through service providers, data of those service providers, content and purpose as well as frequency of inquiries and content of the information provided.

- Technical data of the mobile devices used for data access

Information about devices and systems used to access websites or portals and apps or other forms of communication, such as internet protocol addresses (IP addresses) or type and version of the operating system and internet browser, and in addition device identification and promotional identification or location data and other comparable data of the devices and systems used.

- Data regarding user-generated content

Information posted on websites or apps of RBI such as comments or personal posts and photos or videos and similar content.

- Data regarding products and services procured from other companies

Data of products and services procured for you from RBI as well as from RBI affiliates, Raiffeisen Kapitalanlage-Gesellschaft m.b.H., Raiffeisen Immobilien Vermittlung Ges.m.b.H., Raiffeisen Centrobank AG, Card Complete Service Bank AG. Furthermore, products of Kathrein Capital Management GmbH.

That data includes personal data and detailed data of the products, such as nature of the transactions, durations, interest rate, fees, credit and debit and payments in arrears.

If the products procured are instruments of payment, the processed data will include: payment history, incoming and outgoing wire transfers, payer and payee, providers transmitting payment orders, amount, description and payment reference, client references, frequency and type of money transactions; with non-cash payments, the data of the merchants or service providers receiving payment, and information about the transactions executed with them.

Who will receive my data?

Within Kathrein, those offices and employees will receive your data who need it to fulfill contractual, legal and/or regulatory obligations as well as legitimate interests. In addition, contractually bound processors (including but not limited to IT and back office service providers) will receive your data, provided they need that data to perform their respective services. All processors are contractually bound to keep your data confidential and to process said data only as necessary in the performance of their services.

Furthermore, your data regarding your account/portfolio details that becomes known in the course of doing business with us will be transferred as is customary for banking transactions, in particular for purposes and in the interest of the protection of creditors or for the execution of banking transactions (wire transfer and transaction data).

This transfer includes the transfer of data to affiliates or companies of RBI (Raiffeisen Bank International AG) as well as their shareholdings to safeguard legitimate interests, including for purposes of risk control.

On the basis of a legal or regulatory requirement, public authorities and bodies (European Banking Authority, European Central Bank, Austrian National Bank, Austrian Financial Market Authority, Tax Authorities etc.) as well as our bank and financial auditors can be the recipients of your personal data.

Regarding the transfer of data to other third parties, we would like to note that Kathrein as an Austrian financial institution is obliged to comply with the bank's duty to maintain secrecy in accordance with Section 38 BWG (Banking Act) and is therefore required to keep confidential all client-related personal data and facts that we become entrusted with or have access to due to our business relationship. Therefore, we may only pass on your personal data if you have previously released us expressly and in writing from bank secrecy and if we are obligated or authorized to do so on legal or regulatory grounds. Recipients of personal data can be other credit or financial institutions or similar facilities. We transmit data we need to fulfill our business relations with you. Depending on the agreement, those recipients can be correspondent banks, stock exchanges, custodians, credit agencies or other companies affiliated with the bank (on the basis of regulatory or legal obligations).

Additionally, your data can be transmitted to those recipients for which you have given the relevant consent (data processing agreement, release from bank secrecy).

How long will my data be stored?

We will process your personal data, if required, for the duration of our business relationship (from initial contact, to contract fulfillment and termination) and longer in accordance with the statutory requirements for data retention and recording, which are provided in the Companies Act (Unternehmensgesetzbuch, UGB), the Federal Tax Code (Bundesabgabenordnung, BAO), the Banking Act (Bankwesengesetz, BWG), the Financial Markets Anti-Money Laundering Act (Finanzmarkt-Geldwäschegesetz, FM-GwG), and the Securities Supervision Act (Wertpapieraufsichtsgesetz, WAG).

IP addresses are stored in case of civil claims in accordance with Section 1489 ABGB (General Civil Code) for three years after collection.

In addition, the length of storage will be based on the statutory regulations regarding the statute of limitations which as set forth in the Austrian Civil Code (ABGB) can be up to 30 years in certain cases (in practice, the most relevant statute of limitations is 3 years).

What data privacy rights to I have?

You have the right to access, correct, delete and restrict processing of your stored data, the right to object to processing as well as the right to data portability in accordance with the provisions of the data protection law. Complaints can be directed to the Österreichische Datenschutzbehörde, Wickenburggasse 10180 Vienna, www.dsb.gv.at

Am I obliged to provide data?

In the course of doing business with us you are required to provide the personal data that is necessary for initiating and conducting our business relationship and which we are legally obligated to collect. As a general rule, if you do not provide that data, we will reject entering into the agreement or executing the order, or we will no longer be able to fulfill an existing contract and will have to terminate it. You are however not required to give your consent to the processing of data that is not relevant or not necessary from a legal or regulatory perspective to fulfill the contract.

Is there automated decision-making?

On principle, we do not use fully automated decision-making in accordance with Article 22 GDPR for establishing and fulfilling our business contracts. If we use this process on an individual basis, we will inform you separately, if required by law.