PRIVACY NOTICE

FOR CLIENTS AND BUSINESS PARTNERS

Mizuho Trust & Banking (Luxembourg) S.A.

Last update: March 2025

1. Introduction

In accordance with article 13 of the General Data Protection Regulation ("GDPR"), Mizuho Trust & Banking (Luxembourg) S.A. (the "Bank", "we"), as data controller may process, by electronic or other means, the personal data supplied by its clients or business partners, including, but not limited to, their representatives, contact points, authorized agents, proxy holders or beneficial owners (the "Data Subjects").

The current Privacy Notice describes to Data Subjects how their personal data are collected and processed in the context of their contractual relationship and provides further explanation on the purposes, legal basis, sharing and transfer of personal data, as well as rights that Data Subjects have in relation to their personal data.

We may update this notice from time to time, and in such case publish the latest version on the Bank's website. If you have questions, please seek additional information from the Bank's Data Protection Team (personal.data@mizuho.lu).

2. What are the applicable legal basis, processing purposes and categories of personal data?

Business partners *(e.g. consultants, office visitors or points of contact of suppliers, audit firms and other service providers)*		
Legal basis	**Processing purpose**	**Personal data**
Contract performance (article 6(1)(b) GDPR)	• Entering or performing a contractual relationship between the Bank and Business Partners, such as advisory / audit services to the bank, suppliers of products, goods or services, on-site support from consultants)	• Identity and personal information (e.g., name, surname, gender) • Contact information (e.g., email address, telephone number) • Professional information (e.g., title, qualifications and competences, CV)
Legal obligations (article 6(1)(c) GDPR)	• Perform relevant checks to comply with anti-money laundering and financing of terrorism rules	• Identity and personal information (e.g., ID and passport) • AML/KYC information (e.g. criminal record)
Legitimate interest (article 6(1)(f) GDPR)	• Assurance of security of the Bank's facilities and assets, via visitors register and surveillance cameras (please also refer to the dedicated "Office Visitors and CCTV Privacy Notice" available at the reception, as well as within the website) *(also based on legal obligations)* • Normal course of the Bank's business (e.g. administrative, accounting and corporate purposes, maintain contact with the Data Subject or to develop the Bank's services) • To facilitate the evaluation, negotiation, or completion of a corporate transaction, such as a business sale, merger, or transfer of assets or services	• Security information (e.g., access control related information, CCTV footage) • Identity, contact and professional information • Any type of data deemed strictly necessary in the context of corporate transactions based on a case-by-case evaluation

Clients		
Legal basis	**Processing purpose**	**Personal data**
Contract performance (article 6(1)(b) GDPR)	• Entering or performing a contractual relationship between the Bank and the Client (including, manage Client relationship, manage accounts and credit balances, manage the Bank's products and related services, execute banking operations of any nature, performing fund administration, global custody and security agency services)	• Identity and personal information (e.g., name, surname, gender) • Contact information (e.g., email address) • Financial information (e.g., personal data pertaining to investors in investment funds, banking details, invested amounts,)
Legal obligations (article 6(1)(c) GDPR)	• Purpose of prevent abuses and fraud, as well as complying with legal obligations, notably with applicable anti-money	• Identity and personal information (e.g., ID and passport)

	laundering and financing of terrorism rules, and with applicable national and international sanctions lists and embargos	• AML/KYC information (e.g. criminal records and information collected via other means, such as World check and other third party databases relevant for the activity of the Bank)
Legitimate interest (article 6(1)(f) GDPR)	• To monitor and secure communication channels by recording phone conversations • To carry out statistics and tests, and to develop commercial offers for equivalent products or services (indirect marketing) • To run our business, including managing contractual relationship, meeting administrative accounting and corporate rights and obligations, including the Hermes Reporting Application • To ensure internal quality and risk management • To manage litigation and debt recovery • To facilitate the evaluation, negotiation, or completion of a corporate transaction, such as a business sale, merger, or transfer of assets or services	• Security information (e.g., records of telephone conversations) • Identity, contact, financial and professional information • Any information needed in the context of litigation of debt recovery • Any type of data deemed strictly necessary in the context of corporate transactions based on a case-by-case evaluation

3. Transfer of personal data to third parties

Personal data will not be transferred to any third parties, except to entities required for the performance of the processing of personal data for the aforementioned purposes. To this end, the Bank may transfer personal data to external service providers, auditors, legal advisors, affiliates, corporate transaction counterparties or other entities at Bank group level (the "Recipients").

In such cases, the Bank ensures that relevant Recipients process personal data only in accordance with dedicated instructions and/or based on adequate privacy and data protection measures and contractual framework. The Recipients are generally located in the European Union or in countries outside of the European Union, such as Japan, ensuring an adequate level of protection of personal data. If not, the Bank and the Recipients put in place appropriate transfer safeguards, such as EU standard contractual clauses to ensure the relevant personal data is adequately protected.

4. Transfer of personal data to authorities

To the extent required by applicable law, personal data may also be transferred to judicial and/or administrative authorities. In accordance with applicable legal and regulatory tax provisions pertaining to the automatic exchange of information, personal data may also be disclosed to the Luxembourg tax authorities, which in turn may, acting as data controller, disclose it to foreign tax authorities.

5. Personal data retention period

Personal data will be stored for the longest of the following periods: (i) as long as is necessary for the purpose of which it was collected, (ii) any retention period that is required by law or (iii) the end of the liability period in which litigation or investigations might arise in respect of our services and business. After the applicable retention period(s) have expired, personal data will be deleted or anonymized.

6. Personal data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We limit access to your personal data to those employees, agents, contractors and other third parties on a need-to-know basis, i.e. who need the access for the abovementioned purposes.

Our IT systems are protected against unauthorised access with various level of controlled and password protected access rights.

When transferring or disclosing your personal data the safety measures vary based on the sensitivity of the data and may include e.g. strong identification of the recipient and encryption of the transferred information.

Any special category of personal data, will usually be used separately from other personal data, and access rights to such sensitive personal data are granted only with weighty reasons to stakeholders authorized to process such data for the above-mentioned purposes.

We have implemented procedures to deal with any actual or suspected data security breach and will notify you and any applicable authority about breach where we are legally required to do so.

We are avoiding personal data collection and usage in paper format. If so required, the paper documents and copies will be always stored in locked-up premises.

Our IT organisation together with our Data Protection Team monitor the safety and integrity of the personal data protection on regular basis and have implemented technical measures to prevent and detect any safety breaches that may threaten your personal data.

7. Your rights in respect of your personal data

Each Data Subject has a right to access his/her personal data and may ask for such personal data to be rectified when it is inaccurate or incomplete. Each Data Subject also has a right to be informed and to object to the processing of such personal data, to ask for erasure of such Personal Data, to ask for data portability and for the limitation of processing of such personal data.

In relation thereto, the Data Subject may exercise the above rights by writing to the Bank Data Protection Team (personal.data@mizuho.lu). The Data Subject also has a right to lodge a complaint with the Luxembourg data protection supervisory authority, the National Commission for Data Protection (CNPD).