

Disclosure of Client Data

Information on Disclosure of Client Data for Transactions and Services

There are a growing number of laws, regulations, contractual and other provisions, industry practices, as well as compliance standards, requiring us to disclose client data, when providing certain types of financial services. Article 12 of our General Terms and Conditions (GTC, edition January 2026) establishes the contractual basis for such disclosures in our relationship with you. This document provides you with further details. It supplements the information document (*Information from the SBA regarding the disclosure of client data and other information in international payment transactions and investments in foreign securities*) issued by the [Swiss Bankers Association](#).

1. Why do we need to disclose client data?

Adherence to applicable laws, regulations, licensing conditions, contractual provisions, industry practices and compliance standards is a prerequisite for doing business. This may include the disclosure of certain client data to relevant third parties on a regular basis (e.g.; trade reporting to an exchange) or on specific request (e.g.; unusual transactions).

Affected transactions and services include in particular securities transactions and custody (including corporate actions and transactions involving securities traded in a foreign country where local investor or tax ID is required), payments, foreign exchange transaction, derivatives, precious metal and commodities.

2. Who might receive your client data?

Recipients may be, but are not limited to banks, brokers, exchanges, securities trading platforms, trade repositories, system operators, processing units, clearing houses, custodians, central securities depositories and issuers, depending on the type of transaction and service and the specific involvement of that third party. The receiving third party may also be a UBS branch or affiliate.

Recipients may also be foreign regulators, foreign authorities and their representatives.

3. Which client data might be disclosed?

Disclosed client data may include information on for example:

- Clients, authorized representatives, beneficial owners (any natural person[s] who ultimately owns or controls the [end] client

and/or the natural person on whose behalf a transaction or activity is being conducted) and other involved parties (including, for example, their name, address, domicile, nationality, ID, passport number, contact details)

- Transactions or services (e.g. source of funds and other background information on transactions and services and any other compliance-related information, including client status, client history and scope of the client relationship with UBS)

4. When and how will client data be disclosed?

Disclosure may be required before, during or after the performance of transactions and services, may even occur after the banking relationship has ended and include data relating to transactions entered into and services rendered before the GTC dated January 2026 came into effect. UBS determines in each case which client data is appropriate in the context of disclosure. Recipients may receive client data through any means or channels deemed appropriate including encrypted or unencrypted e-mail.

5. How will disclosed client data be protected?

Recipients of client data are subject to the legal and regulatory data protection standards applicable in the jurisdictions where they operate. Please note that once the client data has been disclosed, it is no longer under UBS's control and you should assume, for practical purposes, that it is also no longer protected by Swiss data protection and banking secrecy law. Recipients of client data within UBS Group are bound by UBS's global information security standards.

UBS does not necessarily know and may have no influence as to how the client data will be used following its disclosure. Normally, local laws and regulations provide what the data may be used for, for example, for combating money laundering, terrorism financing and corruption; for ensuring compliance with local securities laws or for investigating suspicious transactions. However, the data disclosed may eventually be used also for purposes that go beyond what is strictly required by law or regulation.