How we use data

Edition: October 2021

This information relates to our institutional markets business. Please visit www.ubs.com/ibterms

How we use data

Data types

When interacting with our clients, we accumulate data. It broadly falls into the following categories:

Client data

Data our clients give us about themselves, their personnel, their investments and strategies, and investment objectives.

Client-identifying data

Data we hold (which need not be client data) that identify a client or its personnel.

Interaction data

Data we gather when our clients interact with us or use our services.

Transaction data

Data we gather when we handle transactions for or provide services to our clients.

Client data

It's confidential

We take client confidentiality very seriously, and we have policies, processes and controls to support that commitment. We have updated our Code of Conduct and adopted a set of internal principles for the appropriate use of customer data in financial services which we believe reflect excellent practice. We will review any new proposals to use client data by reference to the Code and principles. You can find the UBS Code of Conduct here.

Service enhancement

We continuously seek to better understand our clients' interests and anticipate their needs. To do this, we use each client's own data to customize and enhance our services and product offering for that client. We may confidentially share client-identifying data with our affiliates and third-party service-providers (including those who produce market share surveys) to help us analyse how we are meeting our clients' needs and, where required, with regulators.

Interaction and transaction data

Interaction data

We capture interaction data every time we contact you or you contact us and use it to tailor our services and products to our clients, to provide them with more interesting and relevant content, to evaluate our relationships and to better understand their needs.

Regulatory disclosure

In connection with our role as a regulated provider of financial services, we are required to disclose certain transaction data (which may identify clients) to regulators and operators of market infrastructure under market conduct, anti-money laundering, and other securities regulations in many jurisdictions. We generally describe these regulations in the annex at the end of this disclosure.

Anonymized, aggregated data

We use aggregated and anonymized transaction and interaction data to create data sets that we use for a variety of internal and commercial purposes, including in our Data Solutions business. We apply rigorous controls and methodologies to ensure these data sets do not disclose any client-identifying data.

Information security

Approach

We maintain and enforce comprehensive policies and procedures to secure client data against physical and cyber threats.

Direct and remote access to our systems is governed by enterprise-approved secure authentication and monitored for unauthorized information processing activities. We operate robust firewalls and run a full range of sophisticated security software across our IT infrastructure to prevent, detect, and remediate unauthorized access.

We apply a "clear desk/clear screen" policy to protect against unauthorized access, misuse or corruption of client data.

Our personnel receive regular training on the importance of safeguarding client data and the policies and procedures preventing the improper use of this information within UBS and outside.

Information barriers

Many of our business units operate behind information barriers. These business units may, with approval from the appropriate control functions, share client data with other parts of UBS on a need-to-know basis to appropriately manage our risk and enhance our service to you. The business units cannot otherwise share client information outside those information barriers.

Electronic trading

Our electronic trading businesses use information barriers to safeguard client order information to avoid improper disclosure both internally and externally. Live electronic trading order information remains anonymous, confidential and segregated from other UBS Global Markets businesses (unless the client has specifically agreed to disclosure). Live client order information can only be accessed by directly involved trading and sales coverage team and our risk control and operational infrastructure, on a need-to-know basis, to process and risk-manage resulting trading activity.

Execution Hub

Our UBS Execution Hub operates as a distinct trading desk separate from our standard broker service when facing the market. It uses information barriers to avoid improper disclosure of client order information, trade information and trading strategies. Except where an order is transmitted to UBS for execution as broker, this client information remains segregated from our standard brokerage service. It can only be accessed by UBS Execution Hub, control functions and operations personnel, on a need-to-know basis.

Regulations impacting our use and disclosure of data

Anti-money-laundering regulations

Anti-money-laundering regulations require regulated institutions to report certain kinds of information and activity to regulators.

Securities regulations

Securities regulations are designed (among other things) to ensure the maintenance of fair, orderly and transparent markets, prevent market abuse, insider trading and the misuse of material non-public information, and generally prohibit fraud and improper conduct. We have to disclose transaction data and suspicious trading activity to competent authorities under these regulations.

Conduct regulations

As a regulated financial institution in many jurisdictions, we have general obligations to disclose and manage conflicts of interest and act in our clients' best interests.

Personal data regulations

Personal data regulations govern how we hold, store and process "personal data".

Internal policies

We have comprehensive internal policies to ensure a common standard for protection of client data, including detailed guidelines for the processing and handling of personal data. Separately, we have appointed a Group Data Protection Officer to ensure our compliance with data regulations in the jurisdictions in which we operate. Our privacy notice, published here, explains how we use personal data.