

Information Disclosure Booklet

THE PURPOSE OF THIS DOCUMENT IS TO PROVIDE CLIENTS OF J.P. MORGAN (SUISSE) SA (THE BANK) WITH INFORMATION RELATING TO THE DISCLOSURE OF CLIENT DATA, IN SWITZERLAND AND ABROAD

Article 17 of the *Terms and Conditions Applicable to Clients* of the Bank establishes the legal basis for the disclosure of client data in Switzerland and abroad. This document explains the relevant provisions of Article 17 of the *Terms and Conditions Applicable to Clients* and provides examples in this context. It also integrates the information issued by the Swiss Bankers Association (SBA) in the document *Information from the SBA regarding the disclosure of client data and other information in international payment transactions and investments in foreign securities*.

1. WHY DOES THE BANK NEED TO DISCLOSE CLIENT DATA?

There is currently a global trend towards greater transparency in the financial sector. The Bank is subject to increasing laws, regulations, contractual provisions, industry practices and compliance standards requiring the disclosure of client data in the course of the provision of financial services. The purpose of such transparency is generally to prevent money laundering, the financing of terrorism or corruption as well as to enforce sanctions and market conduct rules.

Compliance with the legal and regulatory framework implies the disclosure of certain client data to relevant third parties in Switzerland and abroad. The basis for the disclosure differs from jurisdiction to jurisdiction, according to local conditions and the requirements of the authorities, service providers or other third parties involved in the transactions and services.

2. WHICH CLIENT DATA MAY THE BANK DISCLOSE?

As a rule, the Bank only transmits client data that it deems necessary in the course of the provision of financial services.

Client data that may need to be disclosed varies from case to case and may include the following:

- Information about the client, authorized representatives, beneficial owners, person giving an instruction, investors and other involved parties (e.g. name, address, contact information, nationality, birth date, origin of the funds, or marital status).
- Information relating to a payment order or other transaction, such as for example, the reason for the transaction, context of the transaction, possible suspicion of non-compliance, or information on other similar transactions.
- Any documentation relating to the business relationship between the client and the Bank, including account opening documentation, "Know your customer" documentation, periodic reviews, statements of assets and credit or debit confirmations.

Client data may include information related to third parties, such as shareholders, beneficial owners, directors, representatives, or authorized signatories, about whom you have provided us with data. It is therefore your responsibility to inform these persons of the potential disclosure of information in Switzerland and abroad.

3. WHO MIGHT RECEIVE CLIENT DATA?

Recipients of client data may be service providers, market participants or organisations (such as brokers, banks, trade repositories, processing units and third-party custodians, issuers, administrators, distributors or managers of any financial instruments or products, or their representatives, and credit card issuers), as well as courts, regulatory bodies, other government agencies, financial market supervisory authorities and tax authorities.

The receiving entity may also be a J.P. Morgan entity located in Switzerland or abroad, including in jurisdictions outside of the European Union, such as the United Kingdom, the United States, India, Singapore, China or Japan.

4. IN WHICH SITUATIONS AND TO WHOM DOES THE BANK DISCLOSE CLIENT DATA?

Disclosure obligations vary from jurisdiction to jurisdiction. In addition, new disclosure obligations may arise at any time. In this context, it is not possible to provide an exhaustive list here and the following are only examples of situations in which client data are disclosed to third parties.

4.1 Disclosure in (international) transactions and investments in financial instruments

In general, the disclosure of client data may be required to enable the Bank to execute payment transactions (incoming and outgoing payments), to proceed to the trading and safekeeping of securities and financial instruments, as well as other transactions and services such as foreign exchange transactions, derivatives, precious metals, and commodities.

(A) Payments

During the processing of cross-border or domestic payments (incoming and outgoing), extensive information concerning the ordering client, the recipient and the payment order may have to be disclosed to the banks and system operators involved, both in Switzerland and abroad. This is particularly the case for payments in foreign currencies, but may also concern payments in Swiss francs. The main purposes are to combat tax evasion, money laundering and financing of terrorism, to enforce sanctions, to comply with local requirements in general and/or to allow the transactions to be carried out. The information concerning the ordering client / recipient includes, for example, name, date of birth, nationality, domicile, origin of the assets, duration of the banking relationship, relationship between the ordering client and recipient, and any agency relationships; and, in the case of companies, for example; the business activity, purpose, ownership structure, beneficial owners, organisational structure and number of employees. As regards to the payment order, it may include information such as the reason for and context of the payment, any suspicious compliance- related factors, as well as details of other similar payments. The banks and system operators referred to are primarily the ordering client's and recipient's banks, correspondent banks and operators of payment systems (e.g. in Switzerland SIX Interbank Clearing AG, or SWIFT). It is also possible that those involved in the transaction may transfer the data to third parties, for example to regulators, authorities and/or other third parties in Switzerland or abroad. Additionally, the recipient of the payment order, whether in Switzerland or abroad, may receive information about the ordering client, or vice versa.

(B) Investment in securities

During the processing of transactions involving domestic or foreign securities, and/or financial instruments, in particular domestic securities linked to foreign currencies (e.g. Swiss investment funds with currency classes), and when such securities are held in custody, extensive information may have to be disclosed to the banks, system operators and other third parties involved, both in Switzerland and abroad. The main purposes are to combat tax evasion, money laundering and financing of terrorism, to enforce sanctions, to comply with local requirements in general and/or to allow the transactions to be carried out. The information includes, for example, name, date of birth, nationality and domicile of the investor beneficial owner, ordering client or recipient in the case of securities transactions, origin of the assets, duration of the banking relationship, relationship between the investor, ordering client and recipient, relationship between the investor and the issuer, any agency relationships; and, in the case of companies, for example the business activity, purpose, ownership structure, beneficial owners, organisational structure and number of employees.

(C) Shareholder identification and participation rights in connection with foreign securities

Foreign laws or regulations may provide for an obligation of the Bank as custodian to disclose client information in view of identifying shareholders and allowing them to exercise their shareholder rights, such as voting rights. By way of example, this is the case of the revised Shareholder Rights Directive (SRD II), the European Union (EU) directive, which applies principally to shares of issuers registered in a EU Member State that are admitted to trading on a EU- regulated market. As a result, it may have implications for shares that you hold in your account. Compliance with SRD II imposes the disclosure of certain information to the issuer in a standardized format. The Bank will comply with such obligation via its third party agent, Broadridge Financial Solutions Inc, based in the United States (including any IT service providers of such third party agent), who will have access to the relevant information required to be disclosed under SRD II. The information varies by jurisdiction. It may involve disclosing identification information related to the account holder and/or the beneficial owner and will, as a minimum, include the name, the address, the number of shares held and the identification number for legal entities.

4.2 Disclosure to courts, regulatory bodies and/or other government agencies

(A) The Bank is required and/or authorized to disclose by Swiss or foreign laws or regulations

The Bank may be required in certain circumstances to provide the Swiss Financial Market Supervisory Authority (FINMA) or another Swiss authority with all the information and documentation it requires to carry out its tasks as supervisory authority.

(B) The Bank is required to disclose by a competent domestic or foreign court, regulator or government agency/authority or in response to an inquiry by any competent body

In the course of a request for mutual assistance issued by a foreign authority (e.g. a foreign country's Attorney General), the Bank may be required to disclose client information and documentation such as the client name, account statements and correspondence, etc. to a Swiss judicial authority (e.g. the Office of the Attorney General of Switzerland) who, in turn, may transmit the foregoing information to the requesting foreign authority.

(C) The Bank is required or permitted to disclose under the law or rules of a regulatory body to which the Bank is subject to or of which the Bank is a member

As part of its obligation to immediately report to FINMA any incident that is of substantial importance, the Bank may be required to share client information (e.g. client name).

(D) Disclosure is necessary to safeguard the legitimate interests of the Bank, specifically in order for the Bank to enforce its rights arising out of or in connection with the Bank's relationship with a client

As part of judicial proceedings initiated by a client against the Bank, the Bank may disclose account relationship information required to protect its interests (e.g. correspondence between the client and the Bank or account opening documentation).

4.3 Disclosure within JPMorgan Chase & Co. (the "Group")

Generally speaking, the Bank is entitled to disclose client data to other entities of the Group, in Switzerland or abroad, for the effective internal control and risk management of the Group, including the management of its legal, compliance, credit and reputation risks, and/or to ensure the compliance by the Bank and/or other members of the Group with applicable regulations in or outside of Switzerland. This includes the following scenarios:

(A) Global management of compliance, legal, and reputational risks and monitoring of business relationships and transactions that entail higher risks related to financial crimes, such as money laundering, financing of terrorism, corruption, bribery, tax evasion, sanctions violations or fraud

The Bank shares certain account relationship information (including the client name and the identity of the beneficiary/originator of transactions) with the Group for the purposes of screening transactions and payments (incoming and outgoing) against sanctions lists and any other regulatory or law enforcement agency lists, anywhere in the world, and in situations where a client is linked to a sanctions program requiring subsequent action, including reporting obligations or the blocking or rejecting of funds or transactions.

In cases where questions regarding the compliance of specific account relationships with legal, regulatory and Group standards and/or the prevention of money laundering or the financing of terrorism, the Bank may be required to disclose the names of holders and beneficial owners of account relationships with the Group.

In cases where there is a reputational and/or financial risk for the Bank and the Group arising from the client activity, the Bank may, under certain conditions, share specific account relationship information with the Group, including the name of the account holder and beneficial owner and/or number of a bank account, the total assets and certain indications on transactions, to the exclusion of more detailed information and copies of any documents.

(B) Underwriting and approving credits and monitoring of credit risks for large or complex credit transactions, including identification of substantial borrowings, significant outstanding credit lines, potential default and margin call issues

In the case of credit transactions over a certain size or with a high level of complexity, the Bank may require consultation with and/or approval of subject matter experts or Senior Management outside Switzerland.

Information shared may contain details of the clients, the clients' balance sheets, the structure, use of loan and source of repayment (e.g. through the sharing of credit approval memos).

(C) The occurrence of circumstances that may affect the reputation and legal risks of the Group

In case of material derogatory information and/or the decision to close an account, or due to geopolitical issues, where escalation to Senior Management or the Financial Investigation Unit is required, the Bank may need to share information such as account details, client name, client positions and outstanding loans.

(D) The group's management of cyber and technology risks and overall improvement of data security by leveraging the Group's know-how and resources

Should you request access to, or copies of, your information that are processed or controlled by the Bank through an attachment to an electronic communication, the Group's protection policies require the attachment to be verified for malwares and any other type of threat. As per the Group's processes, the message would be transferred to a team specialized in cybersecurity, located outside of Switzerland, in order to perform the verification.

In addition to the internal control and risk management of the Group, the Bank is also entitled to disclose certain client data to other entities of the Group, in Switzerland or abroad, in the context of the outsourcing of operational, support, middle office activities and similar functions and operations.

4.4 Disclosure to entities of the Group, third party service providers, in Switzerland or abroad

In order to accept certain documents (e.g. Bank's documentation, contracts) to be signed electronically by means an electronic signature provided by a third party service provider located in or outside of Switzerland, including in the United States of America (e.g. DocuSign Inc.), the Bank may be required to share certain client data with said third party service provider and/or an entity or entities of the Group for the purpose of enabling the operation of the electronic signature infrastructure and ensuring that the client can use the electronic signature options provided by the Bank.

4.5 Outsourcing arrangements in place between the Bank and entities of the Group or third party service providers

In accordance with Article 19 of the *Terms and Conditions Applicable to Clients* of the Bank, the Bank has outsourced certain operations and services to entities of the Group or third party service providers. In particular, the Bank has outsourced to:

- SPS Switzerland AG the printing and mailing of client documentation.
- Entities of the Group, the screening of transactions and payments against lists and any other regulatory or law enforcement agency lists.

In addition, the Bank may engage cloud service providers to assist with data processing and hosting. In the event that the cloud service provider is located in a jurisdiction which does not provide the same level of data protection as Switzerland (including in the United States of America), Client data is generally subject to pseudonymisation.

5. WHEN AND HOW WILL CLIENT DATA BE DISCLOSED?

Disclosure of client data may be required before, during or after the performance of transactions or services and may occur after the closing of your account(s) and after the banking relationship has ended.

A recipient may receive data by any means of communication deemed appropriate by the Bank, including electronically.

6. HOW ARE YOUR DATA PROTECTED ABROAD?

Once information about you and your transactions leave Switzerland, it is no longer protected by Swiss law (e.g. Swiss bank-client confidentiality or the Federal Act on Data Protection), but is subject to the laws of the country concerned. Foreign laws and official orders may, for example, require the information to be forwarded to authorities, supervisory bodies or other third parties. Recipients of client data within the Group are bound by our global information security standards.

Recipients of client data within the Group are bound by our global information security standards.

The website <https://privatebank.jpmorgan.com/gl/en/disclosures/emea-important-information> contains detailed information about how the Group uses and discloses your personal data, reasons and legal basis for the usage of your personal data, as well as the safety measures that the Group applies in this context.