

## **PRIVACY NOTICE FOR NATIXIS DIFC BRANCH CLIENTS**

Natixis DIFC Branch ("we", "our", "us", the "Branch") is committed to protecting the privacy and security of your personal data.

This privacy notice describes how we collect and use personal data about clients, prospective clients, and any other person(s) involved in the business relationship, as the case may be, such as authorised representative(s), person(s) holding a power of attorney and beneficial owners (collectively, "clients"), in accordance with the General Data Protection Regulation (GDPR), DIFC Data Protection Law 2020 (DIFC Law No. 5 of 2020) (the "**Data Protection Law**") including the DIFC Data Protection Regulations (the "**Regulations**") and the Kingdom of Saudi Arabia's Personal Data Protection Law, altogether collectively called as the "**Data Protection Legislation**" throughout this document.

Natixis SA and the DIFC Branch are "joint-controllers". This means that we are responsible for deciding how we hold and use personal data about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to clients, prospective clients, and any other person(s) involved in the business relationship, as the case may be. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions along with the Natixis data protection policy ("**the Policy**") (*located here: [Link](#)*) when we are collecting or processing personal data about you, so that you are aware of how and why we are using such information.

### **DATA PROTECTION PRINCIPLES**

We will comply with the Data Protection Legislation. This says that the personal data we hold about clients must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

## HOW WE WILL COLLECT AND USE DATA ABOUT YOU

We collect and otherwise process personal data relating to clients, prospective clients and any other person(s) involved in the business relationship, as the case may be, such as authorised representative(s), person(s) holding a power of attorney and beneficial owners. In connection with a product or service provided to our clients, we may also collect information about their dependents or family members, if different from the client, each an "Affected Person".

We also process - insofar as necessary to provide our services - personal data that we obtain from publicly accessible sources (e.g. press, sanctions lists, internet) or that is legitimately transferred to us by other affiliates of Natixis or from other third parties (e.g. a credit ratings agency, exchanges, and other similar entities. Also, third party service providers such as professional advisers, insurers, dependants or family members).

Clients, before providing Natixis personal data relating to the Affected Persons, should provide a copy of this notice to those individuals.

Relevant personal data is the personal information of a client or Affected Person (e.g. name, address, contact details, date and place of birth, and nationality). It can also include (but not limited to):

- Identification data and authentication data (e.g. passports, social security numbers, sample signature, photographs)
- Data relating to current and past professional roles and employment, and education (e.g. corporate title, membership of professional associations or bodies, career histories, knowledge and experience in investment matters, qualifications and skills)
- Data relating to criminal convictions and offences
- Data related to designation as a politically exposed person (PEP)
- Data from fulfilment of our contractual obligations (e.g. orders or payment transactions)
- Information about a client's or an Affected Person's financial situation (e.g. creditworthiness data, scoring/rating data, origin of assets, source of wealth)
- Data from interactions with us (our branches, our internet websites, our apps, our social media pages, meetings, calls, chats, emails, interviews and phone conversations) together with documentation data (e.g. file notes or meeting minutes from a consultation)
- Marital status, name of spouse, number of children
- Marketing and sales data
- Dietary and access requirements (e.g. for event organization purposes)
- Video surveillance and telephone/ audio recordings
- Data relating to habits and preferences
- Health information
- Other data similar to the categories mentioned.

## THE RATIONALE FOR PROCESSING YOUR PERSONAL DATA

We process personal data in accordance with the Data Protection Legislation

#### **a. For fulfilment of contractual obligations**

Data is processed in order to provide banking and financial services in accordance with our legal agreements with our clients or to carry out pre-contractual measures that occur as part of a request from you.

The purposes of data processing are primarily in compliance with the specific product or service (e.g. credit, securities) and can include needs assessments, advice, discretionary management, asset management and support, as well as carrying out transactions.

Any special categories of personal data (such as health data or criminal records) will be processed in line with the additional obligations for such personal data under the Data Protection Legislation.

#### **b. In the context of legitimate interests**

Where required, we process your data beyond the actual fulfilment of the contract for the purposes of the legitimate interests pursued by us or a third party provided such interests are not overridden by your rights or interests. Examples include:

- Consulting with credit rating agencies to investigate creditworthiness and credit risks
- Reviewing and optimising procedures for needs assessment for the purpose of direct client discussions
- Marketing (whether direct marketing or any other form of marketing) or market and opinion research (which may include profiling), unless you have objected to the use of your data
- Obtaining personal data from publicly available sources for client acquisition purposes
- Measures for business management and further development of services and products
- Risk control in Natixis
- Asserting legal claims and a defense in legal disputes
- Natixis' IT security and IT operation
- Prevention and investigation of crimes
- Video surveillance and measures to protect the rights of an owner of premises to keep out trespassers and to provide site security (e.g. access controls).

#### **c. As a result of your consent**

As long as you have granted us consent in accordance with the Data Protection Legislation to process your personal data for certain purposes (e.g. analysis of trading activities for marketing purposes or an invitation to an event), this processing is legal on the basis of your consent. Consent given can be withdrawn at any time by notifying us using either of the contact methods set out under the heading "Who is responsible for data processing & how can I contact them?" below, and does not affect the legality of data processed prior to withdrawal.

#### **d. Where necessary for compliance with Applicable Law**

We are authorised and regulated by the Dubai Financial Services Authority ("DFSA") for the conduct of Financial Services in and from the DIFC.

As a financial services firm, we are subject to various legal obligations under the applicable laws (e.g. money laundering, terrorist financing or other financial services laws, regulations, rules, the Financial Services and Markets Act 2000, MIFID and any tax or sanctions laws, regime, treaty or directive). The purposes of processing include assessment of creditworthiness, identity and age checks, fraud and money laundering prevention, fulfilling control and reporting obligations under financial regulation, and measuring and managing risks within Natixis.

### **If you fail to provide personal information**

In the context of our relationship, you must provide all personal data that is required for accepting and carrying out a business relationship and fulfilling the accompanying contractual obligations or that we are legally obliged to collect. Without this data, we are, in principle, not in a position to enter into a legal agreement with you to provide banking and financial services.

In particular, anti-money laundering regulations require us to identify you on the basis of your identification documents before establishing a business relationship and to collect and put on record name, place and date of birth, nationality, address and identification details for this purpose.

In order for us to be able to comply with these statutory obligations, you must provide us with the necessary information and documents in accordance with applicable anti-money laundering regulations, and to immediately disclose any changes over the course of our relationship. If you do not provide us with the necessary information and documents, we cannot enter into or continue the business relationship you require.

### **Change of purpose**

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason which is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent where required or permitted by the Data Protection Legislation.

### **What is “Special Categories of Personal Data”?**

Special Categories of Personal Data are personal data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.

### **How we use Special Categories of Personal Data**

Special Categories of personal data require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data. We have the Policy and safeguards which we are required by law to maintain when processing such data. We may process Special Categories of Personal Data if one of the following conditions are met:

- With your explicit written consent;
- if the processing is necessary for us or for you to carry out our/your obligations or exercise our/your rights in the context of your employment;
- if the processing is necessary to protect your vital interests or another natural person where you are unable to give consent;

- if processing relates to personal data made public by you;
- if the processing is necessary in connection with legal claims;
- if the processing is necessary for compliance with laws to which we are subject (provided we have given you clear notice of such processing as soon as reasonably practicable unless this is prohibited);
- if the processing is necessary for compliance with anti-money laundering or counter-terrorist financing obligations or the prevention, detection or prosecution of any crime;
- if the processing is necessary for public health reasons or to assess the working capacity of an employee;
- if the processing is proportional and necessary to protect you from potential bias or inaccurate decision making; and
- if the processing is necessary for reasons of substantial public interest that are proportionate to the aim(s) pursued provided your rights are safeguarded.

## **AUTOMATED DECISION-MAKING**

We do not envisage that any decisions will be taken about you using automated means. If we use this procedure in individual cases, we will inform you of this separately, provided it is a legal requirement to inform you. You have a right to object in certain instances where a decision is taken by us based only on automated decision making and to require such decision to be reviewed manually.

## **PROFILING**

We process some of your data automatically, with the goal of assessing certain personal aspects (profiling). For example, we use profiling in the following ways:

- Due to legal and regulatory requirements, we are required to combat money laundering, terrorism financing, fraud, and assess risk and offences that pose a danger to assets
- Data assessments (including on payment transactions) are also carried out for this purpose. At the same time, these measures also serve to protect you
- Assessing credit worthiness in relation to provision of lending products
- We use assessment tools in order to be able to specifically notify you and advise you regarding products.
- These allow communications and marketing to be tailored as needed, including market and opinion research.

## **DATA SHARING-DISCLOSURE TO THIRD PARTIES**

The following paragraphs set out details of where we transfer client personal data to and the purpose for any such transfer:

### **a. Natixis**

We will share your personal data with affiliates of Natixis, including outside of the DIFC. We will transfer your personal data to achieve the purposes described under the heading, “How we will use Your Data”.

We may also pass on information about you to any of our affiliates in connection with any services that we think you may be interested in.

#### **b. External recipients of data**

We will transfer personal data about you in the course of conducting our usual business, or if legal, regulatory or market practice requirements demand it to the following external recipients, or if you have given your consent (e.g. to process a transaction you have ordered us to fulfill):

- To public entities and institutions (e.g. authorities such as the Dubai Financial Services Authority, the Central Bank of the UAE, the DIFC Registrar of Companies, the Prudential Regulation Authority, Financial Conduct Authority, other supervisory authorities and law enforcement agencies) either upon providing a legal or regulatory request or as part of our legislative and regulatory reporting requirements
- To other credit and financial service institutions or comparable institutions in order to carry out a business relationship with you (depending on the contract, e.g. correspondent banks, custodian banks, brokers, stock exchanges, credit rating agencies)
- To third parties (for example correspondent banks, brokers, exchanges, trade repositories, processing units and third-party custodians, issuers, authorities, and their representatives) for the purpose of ensuring that we can meet the requirements of applicable law, contractual provisions, market practices and compliance standards in connection with transactions you enter into and the services that we provide you with
- To a natural or legal person, public authority, agency or body for which you have given us your consent to transfer personal data to or for which you have released us from banking confidentiality.

#### **c. To service providers and agents**

We will transfer your personal data to service providers and agents appointed by us for the purposes given, subject to maintaining banking confidentiality. These are companies in the categories of banking services, IT services, logistics, printing services, telecommunications, collection, advice and consulting, and sales and marketing.

We will implement appropriate organisational and technical safeguards to protect the personal data for which it acts as data controller at all times.

#### **Transferring information outside the DIFC**

Data transfers to legal entities outside the DIFC and jurisdictions with data protection legislation deemed adequate or equivalent by the DIFC Commissioner of data Protection (the "Commissioner") (together known as "third countries") takes place so long as:

- The third country has been determined by the Commissioner as jurisdiction providing adequate level of protection under the DIFC DP Law
- We have provided appropriate and suitable safeguards under the DIFC DP Law and enforceable data subject rights and effective legal remedies for data subjects are available
- One of the specific derogations in the DIFC DP Law (Article 27(3)) applies (including, but not limited to, where you have explicitly consented to the proposed transfer in accordance with the DIFC DP Law) or
- The limited circumstances set out in the DIFC DP Law (Article 27(4)) apply.

You understand that the data protection legislation outside the DIFC may not give you as much protection as the data protection legislation inside the DIFC.

Please contact us if you would like to request to see a copy of the specific safeguards applied to the export of your information.

## DATA RETENTION

### For how long will my data be stored?

We will process and store clients and Affected Persons personal data for as long as it is lawful for us to do so.

We will normally retain your records for a minimum of six years from, for example, the time the client relationship comes to an end, to comply with regulatory and contractual requirements unless there is a particular reason to hold the records for longer, including legal hold requirements, such as in anticipation of litigation, which require us to keep records for an undefined period of time.

## INFORMATION SECURITY

We are committed to protecting your privacy and to keeping your personal data safe. We will ensure that appropriate measures are taken against unlawful or unauthorized processing of your personal data, which is not in accordance with this notice, and to protecting your personal data against accidental loss or damage.

## YOUR RIGHTS

### Your rights in connection with personal data

Under certain circumstances, by law you have the right to:

- **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where data protection laws allow for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- **Request the restriction of processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal data to another party.
- **Data Portability**
- **Right to Object** where applicable, to decisions based solely on automated processing including profiling

- **The right to non-discrimination** if you exercise any rights under the Data Protection Legislation

In addition to the above rights, you have the right to object at any time to:

- On reasonable grounds relating to your particular situation, the processing of your personal data for the reasons set out in “The rationale and legal basis for processing your data” (in the context of legitimate interests) of this statement above (including profiling for these purposes), to the extent permitted under the Data Protection Legislation.
- The processing of your personal data for direct marketing purposes, and profiling to the extent related to direct marketing
- Your personal data being disclosed to third parties as set out under “data sharing disclosure to third parties” or used on their behalf for the purposes of direct marketing.

You may also withdraw consent granted to us for the processing of your personal data at any time. Please also refer to “As a result of your consent section” of this statement above, for further details on consent.

Any requests in relation to exercising your data privacy rights do not need to be made in a particular form however, it should be addressed to us using either of the contact methods set out under the heading “Contact Details” below.

## **CONTACT DETAILS**

If you have any questions about this privacy notice or our processing of your how we handle your personal data, please contact us at;

### **Attention: Data Protection Officer**

Natixis (Dubai Branch)  
ICD Brookfield Place  
Level 10, Unit 2,  
P.O. Box 506694  
Dubai, U.A.E.

E-mail : [dpo@natixis.com](mailto:dpo@natixis.com)

## **CHANGES TO THIS PRIVACY NOTICE**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may provide updates from time to time to this privacy notice by clicking here [\[Link\]](#)