NATIXIS

Update 18 May 2018

INFORMATION NOTICE CONCERNING PERSONAL DATA

The BPCE Group is made up of the following Natixis legal entities and branches in Europe in relation to our corporate and institutional banking business:

FRANCE:
Natixis - 30 avenue Pierre Mendès-France, 75013 Paris – Postal address: BP 4 – 75060 Paris Cedex 02
Tel: +33 1 58 32 30 00 - www.natixis.com
Société anonyme with share capital of €5,019,776,380.80 – 542 044 524 Paris Trade & Companies Register

UK:
Natixis, London branch, Cannon Bridge House, 25 Dowgate Hill, London, EC4R 2YA Tel: +44 020 3216 9000

GERMANY:
Natixis Zweigniederlassung Deutschland - Im Trutz Frankfurt 55 - 60322 Frankfurt am Main -Tel: +49 69 97153 0

ITALY:
Natixis S.A. Milan Branch Via Borgogna, 8; I-20122 MILANO MI Tel. +39 02 0066 7200

SPAIN:
Natixis SA, Sucursal en España - Serrano 90, 5th floor - CP 28006 Madrid Tel: +34 91 111 77 00

The following Information Notice applies to the business relationship between you and the above Natixis entity(ies) hereinafter referred as 'Natixis'.

On the basis of the information requested by our employees, agents or distributors, forms completed by our you, automated data capture mechanisms or information gathering processes more generally, **Natixis** as **data controller** collects and processes information that allows individuals to be identified and may concern their private or professional lives (for example, their name, date of birth, private or professional contact details, family circumstances, photograph, identity documents, occupation etc.).

Such information is referred to below as "**Personal Data**" **or** "**Data**".

Protecting **Data** is essential in order to build a trusting business relationship.

To this end, **Natixis** constantly monitors its compliance with the law[1] on the protection of **Personal Data** and aims to ensure responsible governance of its information files as well as maximum transparency of the **Data** processing it carries out.

Natixis has appointed a **Personal Data Protection Officer** (or DPO). This person ensures that **Natixis**'s processing of Personal Data complies with the applicable regulations.

This information notice has been sent to you as an individual affected by Natixis's data processing. It explains why Natixis SA needs to collect your Data, how your Data will be used and protected, how long it will be retained and the rights that you have.

Whose Data is collected?

Our customers and their legal representatives, agents, contact persons, staff or beneficial owners, as applicable.

[1] ***General Data Protection Regulation no. 2016/679 of 27 April 2016 and applicable Data national laws***

What Data does Natixis use and where does it come from?

Natixis collects and uses Data that is strictly necessary for its activities and for the purposes set down in this information notice.

Categories of Data used:

- **Identifying data** (e.g. marital status, identify card/passport, nationality, place and date of birth, sex, address, pictures),
- **Contact details** (e.g. postal address, email, telephone),
- **Data on personal life** (e.g. family circumstances),
- **Data on professional life** (e.g. occupation, name of employer),
- **Economic and financial information** (e.g. income, financial position, tax position, tax identification number, bank account details, transfers etc.),
- **Connection data** (e.g. IP address, logs, etc.),
- **Data about your habits and preferences** in connection with the use of our products and services, as resulting from our interactions (websites, applications, discussions, etc.).

Sensitive categories of Data:

Natixis does not process Data in connection with racial or ethnic origin, political opinions, religious or philosophical convictions or trade union membership, genetic, biometric or health data, data on sexual life or sexual orientation or data concerning criminal convictions or convictions for misdemeanours, unless necessary and required or permitted under applicable legislation.

Sources of Data:

The Data used by Natixis has been supplied directly by you or has been obtained indirectly via our business and institutional customers, our partners or public sources.

Direct collection:

- Data consciously provided by you (e.g. via a questionnaire or orally),
- Data collected by Natixis through observation of the person concerned (e.g. automated data capture tools or software, WiFi tracking).

Indirect collection:

- Data obtained via the Banques Populaires et Caisses d'Epargne group for custody account holders;
- Data from official public sources (e.g. official gazette) or public databases;
- Data from websites and social media made public by you;
- Data obtained via our business and institutional customers (e.g. data supplied by a customer about its beneficial owners);
- Data obtained via our service providers (e.g. businesses supplying Data in relation to fraud).
-

On what basis is your Data collected and used and for what purposes?

As part of our banking relationship, **Natixis** needs to gather your **Data** for the purposes described below, on the basis described:

- **Performing the contracts for the products and services you have taken out or wish to take out:**

  For **Natixis,** this means:
  - Managing the accounts, products and services (including any financial instruments) taken out by you or by our business and institutional customers (of whom you are a staff member, shareholder, beneficial owner or customer – for instance, in relation to cash management),
  - Managing transactions and associated cash flows,
  - Providing virtual content, information and recommendations (for instance in relation to capital markets),

- Providing assistance and handling your requests in this regard.

Unless it can gather and process your Data, **Natixis** will not be able to make or perform the contracts that bind us to our customers and counterparts.

- **Fulfilling our legal and regulatory obligations**

Natixis must gather your Data in order to meet its obligations:

- In relation to banking and financial matters:
  - Putting security measures in place to prevent fraud, for instance to detect abnormal transactions, in relation to embargoes and more generally to combat financial crime both in respect of the financial sector and in respect of Natixis, its customers and its staff,
  - Monitoring and reporting on the risks that institutions may run,
  - Recording telephone conversations and written messages (electronic and instant messaging) in connection with transactions on the markets,
  - Meeting its obligations to report to any competent public or judicial authorities and to answer any official request issued by a competent public or judicial authority,
- In relation to the prevention of money laundering and terrorist financing,
- In relation to the prevention of tax evasion, including reporting obligations vis-à-vis the authorities,
- In relation to market abuse,
- In relation to transparency and the prevention of corruption,

Otherwise, **Natixis** will not be able to continue its business relationships with its customers or counterparts.

- **Where Natixis SA has a legitimate interest in using your Data**

Natixis may process your Data on the basis of its "legitimate interest" if it finds itself in a position that could present risks to its business or is required to defend its rights, or in order to develop its products or services. This includes:

- Ensuring the security of its IT systems,
- Defending its rights,
- Managing relations with customers and prospective customers,
- Personalising our product and service offering by segmenting our customers and prospective customers, including by aggregating Data for analytical or anonymisation purposes,
- Improving our products and services,
- Audit and inspection activities.

- **Purposes for which your consent is required**

Natixis intends to make certain types of Data processing subject to obtaining your consent. In such cases, you will be asked to consent specifically to the collection and processing of your Data for expressly stated purposes.

For example, in relation to any direct marketing sent to customers or prospective customers who are individuals, your consent will be required if you are not a **Natixis** customer, or if you are a **Natixis** customer but the sales material relates to products that are not comparable to those you have already taken out.

Description of the purposes for which your Data is used
Managing the accounts, products and services (including any financial instruments) **taken out by you or by our business and institutional customers** (of whom you are a staff member, shareholder, beneficial owner or customer – for instance, in relation to cash management): *For Natixis, this means recording and updating information about account holders and the operating features of their accounts, managing data on the monitoring of activities in relation to financial instruments, and keeping accounts more generally (regular statements, extracts and summaries, transaction stops, issuing cheque books, bank details*

slips and certifications).
Natixis also processes Data needed to provide you with the products and services you request. This includes the making, administration and performance of contracts, as well as providing assistance and handling your requests in this regard.

Managing transactions and cash flows:

For Natixis, this means managing Data about account transactions: deposits and withdrawals (cash, cheques, transfers, direct debits, card transactions and other movements of funds), while managing the quality of sales transactions with our customers in relation to our ISO certification.

This includes trade finance transactions, transaction data exchanged via our portals, transfers and direct debits in euros, electronic money tools and international currency payments more generally, as well as providing assistance and handling your requests in this regard.

Providing virtual content, information and recommendations (for instance in relation to capital markets):

For Natixis, this means enabling you to have secure online access to information whenever you sign up for a product.

Fulfilling our legal and regulatory obligations:

- In relation to banking and financial matters:
    - Putting security measures in place to prevent fraud, for instance to detect abnormal transactions, meet our obligations in relation to embargoes, and to combat financial crime more generally:

For Natixis, this means detecting actions that are carried out in relation to anomalous or inconsistent activities or activities that have been indicated as potentially relating to fraud. Such actions may include, for instance, submitting a false payslip or false proof of identity, providing contradictory information, or inconsistencies in relation to the place of a transaction etc.

The security measures in place also include managing alerts (which involves making verification checks or requesting explanations or documentary evidence) and drawing up lists of persons duly identified as the perpetrators of acts considered to be external fraud or attempted fraud.

    - Recording telephone conversations and written messages (electronic and instant messaging) in connection with transactions on the markets:

Financial markets regulations require Natixis to record all discussions by its traders and bankers, particularly those with customers.

    - Monitoring and reporting on the risks that institutions may run
    - Meeting our obligations to report to, and answer any official request issued by, the competent public or judicial authorities,
- In relation to the prevention of money laundering and terrorist financing:

For Natixis, this means detecting atypical behaviour that may constitute money-laundering transactions and to report such behaviour to the regulators where a strong suspicion exists. This includes collecting personal data about managers, shareholders and beneficial owners.

- In relation to the prevention of tax evasion, including reporting obligations vis-à-vis the authorities:

The automatic exchange of banking and financial information requires financial institutions to have procedures and a systematic data transmission system for non-resident customers.

- In relation to market abuse:

Monitoring transactions by managers in order to detect potential market price manipulation or insider trading.

- In relation to transparency and the prevention of corruption:

Natixis may be required to report its lobbying activities and deal with whistleblowing, including as a whistleblower itself.

Ensuring IT security, defending our rights and developing products or services, including:

- Ensuring the security of our IT systems,

Natixis employs authentication mechanisms and cybersecurity measures that involve processing Data in relation to access to its websites or web applications.

- Protecting our rights:

Natixis may use Data in the context of complaints, disputes, lawsuits, corporate restructuring measures or other merger-related transactions.

- Managing relations with customers and prospective customers:

Natixis keeps a log of its interactions with customers and potential customers, and records and manages sales transactions and marketing campaigns.

- Personalising our product and service offering by segmenting our customers and prospective customers, including by aggregating Data for analytical or anonymisation purposes:

Natixis needs to know its market in order to communicate better with its customers and identify their needs. We aggregate customer Data for reporting and statistical analysis purposes in order to develop our market.

- Audits and inspections.

Audits are carried out by the General Inspection department of Natixis or BPCE with the aim of managing risk and ensuring the compliance of Natixis operations. This may involve processing customer Data.

- **Cookies and other trackers**

By cookies or other trackers we mean trackers that are placed and read, for example, when you open a website, read an email or install an item of software or a mobile app.

When you visit a **Natixis** website, cookies and trackers may be installed on your device (your computer, smartphone, tablet, etc.).

Natixis's cookie policy may be consulted on any of its websites, under the heading "Cookies" in the legal notices section or at the foot of the web page.

Who has access to your Data?

Natixis takes all necessary steps to ensure the safety and confidentiality of the Data it collects, i.e. to ensure that only authorised persons have access to it.

Only persons who are authorised by virtue of their activity in the competent **Natixis** departments that are in charge of the relevant processing have access to your Data, and only within the scope of their authorisations.

BPCE Group companies (subsidiaries and branches), our service providers and our partners may likewise have secure access to your Data insofar as it is needed in relation to the performance of their services or our collaboration agreement.

Your Data will also be passed to certain authorities in accordance with the applicable law and regulations.

In the above circumstances, **Natixis** may transfer your Data (by communicating or making it accessible) to another country either in or outside the European Union.

Your Data may be transmitted to or accessible by:

- Subsidiaries and branches of the BPCE Group in France and abroad:
  - In relation to the sharing of resources, particularly financial and IT resources,
  - In the event of restructuring involving a merger or similar transaction,
  - In relation to operational risk management,
  - In relation to the management of customer relations, investments and transactions (customers of our investment bank) or in connection with the prevention of money laundering and the financing of terrorism,
- IT and financial service providers (IT hosting, technical maintenance and support) in France and abroad,
- Intermediaries, brokers and banking partners in France and abroad,
- Beneficiaries of funds transfers and their banks in France and abroad
- Competent tax, financial, administrative or judicial authorities in France and abroad:
  - French and foreign tax authorities in relation to the prevention of tax evasion;
  - An authorised financial information unit (such as Tracfin in France or UIF-Unità di informazione finanziaria in Italy),
  - French and foreign authorities in accordance with international law and treaties,
  - Competent public authorities in charge of data on persons subject to asset freezing orders (in France, the Direction Générale du Trésor or Autorità Giudiziaria and Agenzia delle Entrate-Riscossione in Italy),
- Certain regulated professions (lawyers, notaries, auditors) in France and abroad,
- The General Inspection departments of BPCE and Natixis

Transfers of Data outside the European Union

Your data may be transferred from an EEA country to a non-EEA country provided that the European Commission has recognised that country as providing an adequate legal level of Data protection with respect to European legislation (e.g. Switzerland, Canada).

Where Data is transferred to countries outside the EEA in which the legal level of Data protection has not been recognised as adequate (e.g. India, China, United States), Natixis will base its transfer:

- on one of the binding legal assurances provided for by the regulations:
  - The signing of contractual clauses of a type approved by the European Commission whereby the recipient of your Data guarantees the protection of your Data,
  - Binding corporate rules applicable by our recipient service providers that guarantee the protection of your data,
- or on one of the exemptions for specific transfer situations:
  - The transfer of Data to the recipient bank is necessary in order to carry out an international payment (transfer necessary for the performance of a contract),
  - The transfer of Data to the authorities in accordance with our legal and regulatory obligations (transfer necessary to safeguard the public interest).

To obtain a copy of these assurances or the location at which they can be obtained, you may contact our Data Protection Officer in the manner described under "How do you exercise your rights?"

How long will your Data be retained?

Most Data collected in relation to a specified customer are kept for the duration of the contractual relationship plus a specified number of years after the end of the contractual relationship.

Our criteria for defining our retention periods are:

- Meeting our operational obligations (e.g. account maintenance, facilitating customer relationship management) and

- Legal requirements (if any).

In case of regulatory requests or legal claims, our retention standards may be increased in this regard for Natixis defense.

What rights do you have over your Data?

Within the limits and conditions laid down by current legislation, you can:

- **Obtain access** to all of your Data,
- **Rectify, update and delete** your Data for legitimate reasons,
- **Object** to the processing of your Data for legitimate reasons and object to the processing of your Data for direct marketing purposes without giving any reason,
- Request the **portability** of your Data for processing that requires your consent or for the performance of a contract that has been or will be made,
- Demand the **limitation of the processing** we perform in relation to your Data,
- **Withdraw your consent** at any time (for processing that requires your consent),
- Lodge a **complaint** with a competent supervisory authority, i.e. the authority in the country of the European Economic Area of your habitual residence, your place of work, or the place of an alleged infringement**:**
  - in **France**, this is the CNIL: www.cnil.fr
  - in the **UK** this is the Information Commissioner Office : www.ico.org.uk
  - in **Germany** this is der Hessische Datenschutzbeauftragte: www.datenschutz.hessen.de
  - in **Italy** this is Garante per la Protezione dei dati personali: www.gpdp.it
  - in **Spain** this is Agencia Española de Protección de Datos: www.agpd.es

How do you exercise your rights?

To exercise your rights, please contact our **Data Protection Officer** by email or by post, stating your full name and contact details, providing a copy of your identity document and specifying Natixis legal entity, branch and country you are in business relationships with.

Data Protection Officer	
Natixis France, UK, Italy and Spain	
Natixis – BP 4 – 75060 Paris Cedex 02 France	dpo@natixis.com
Natixis Germany	
Natixis Zweigniederlassung Deutschland Im Trutz Frankfurt 55 - 60322 Frankfurt am Main	datenschutz-npb@natixis.com

In relation to electronic communications for direct marketing purposes:

An unsubscribe link (for emails) or a unsubscribe number (for SMS/MMS messages) also appears on every electronic message sent to you by **Natixis**.

Country specific provisions:

France:

You also have the option of sending us instructions concerning the retention, deletion and communication of your Data after your death. These instructions may also be registered with a "certified digital trusted third party". Such instructions, a kind of "digital will", may designate a person in charge of their execution; failing this, your heirs will be designated.

Spain:

The legal heirs of a deceased person may contact us in order to request access to the personal data of that person and, where appropriate, rectification or deletion.
As an exception, the heirs may not access the data of the deceased, nor request its rectification or suppression, when the deceased had expressly prohibited it or so established by law.
The testamentary executor as well as that person or institution to which the deceased had expressly designated for this purpose may also request, in accordance with the instructions received, access to the personal data of the latter and, where appropriate, its rectification or suppression.