

## EMPLOYEES INFORMATION NOTICE REGARDING PERSONAL DATA

Employers' compliance with the rules regarding personal data protection contributes to transparency and trust vis-à-vis their employees.

Throughout the employee's life cycle, your employer **Natixis SA in France or one of its affiliated company in France, excluding Natixis Investment Managers and affiliates (hereinafter 'Natixis')** will collect, use and store a significant amount of information which identifies you personally and may concern both your private and professional life (for example, your name, date of birth, personal or business contact information, family situation, photograph, occupation, etc.).

This information is referred to hereinafter as '**Personal Data**' or '**Data**'.

Natixis continuously ensures compliance with the legal rules<sup>1</sup> on the protection of **Personal Data** and strives to ensure responsible governance of its electronic or other files (paper documents) as well as the highest degree of transparency with respect to **Data** processing.

To this end, you will be made aware and, depending on your position, receive in-depth training on the subject of "Personal Data Protection".

Natixis has appointed a **Data Protection Officer** (or DPO) whose contact information can be found in the internal directory. This person independently ensures that the processing of Personal Data implemented by Natixis, particularly in terms of human resources, complies with applicable regulations.

This memorandum explains why Natixis 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.

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

During the term of your employment contract, **Natixis** will collect and use Data – in addition to the information collected when you submitted your application – as absolutely necessary for its activities and strictly for the purposes described in this memorandum.

**Recruitment:** Name and address, social security number, bank details, employment contract, diplomas, image rights authorisation, family situation, contact information, etc.

**Work:** internal directories, business continuity plan, organisation charts, video surveillance data, badges, amendments to the employment contract, supporting documents (medical, expenses, etc.), surveys, business travel, computer and telephone supplies and resources, application connection (logs, IP address) and access data, absences, leave, medical records, protection and mutual insurance, lunch vouchers, declarations of interests, staff movement logistics, etc.

**Payroll:** Payslips, social contribution declarations containing names, disability rate, etc.

**Evaluation and Training:** Annual evaluations, training courses, career file, professional interview, etc.

**Termination:** letter of retirement, letter of resignation, final account statement, contractual termination, dismissal notice, etc.

---

<sup>1</sup> \* *General Data Protection Regulation 2016/679 of 27 April 2016 and French Data Protection Act (loi Informatique et libertés 78-17 du 6 janvier 1978 amended)*

## Categories of sensitive Data

Natixis does not process Data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic, biometric or health-related data, sex life or sexual orientation, criminal convictions and offences, unless necessary and required or permitted by applicable legislation (e.g. occupational health, authorised biometric devices, trade union membership during elections of staff representatives).

### Data source:

The Data used by Natixis was provided directly by you or was obtained indirectly via our corporate and institutional clients, our partners or public sources.

### Direct collection:

- Data provided knowingly by you (e.g. via a questionnaire or verbally),
- Data collected by Natixis by observing the person in question (e.g. automated data capture tools or software, WiFi tracking, evaluation by your managers).

### Indirect collection:

- Data obtained via other employees;
- Data obtained via the Banques Populaires and Caisses d'Epargne network in case of internal move.

## For what purposes, on what grounds and for how long is your Data retained?

As part of our work relationship, Natixis needs collect and retain your Data for specific purposes and as long as necessary to achieve those purposes, taking into account any obligations to retain certain Data.

Some Data may be required by law or to perform the contract of employment.

The below table specifies the purposes and legal grounds for Data processing.

| Macro-purpose                                      | Sub-purpose   | Legal basis   |
|--|---|---|
| <b>Career, performance and training management</b> | Career management (professional and skills evaluation and professional mobility management)   | Contractual basis<br>Legitimate interest                      |
|  | Training management (tracking of requests, training courses taken or to be taken, organisation of training sessions, skills and training assessments)                 |   |
| <b>Administrative personnel management</b>         | Administrative management of employee records (arrival documents, employee profile and employee-related documents) in accordance with applicable laws and regulations | Contractual basis<br>Legal obligations<br>Legitimate interest |
|  | Management of employees' administrative requests  |   |
|  | Employee surveys  |   |
|  | Single Employee Register  |   |

| Macro-purpose  | Sub-purpose   | Legal basis                              |
|--|---|--|
| <b>HR reporting</b>                                    | Reports needed to manage HR activities (headcount, industrial relations, diversity, training, career management) and comply with legal and regulatory requirements                                      | Legal obligations<br>Legitimate interest |
| <b>Temporary employment management</b>                 | Temporary employment requests, selection of profiles by temporary employment agencies, sending the temporary employment contract, management of invoicing for temporary employees + statistical reports | Contractual basis<br>Legitimate interest |
| <b>Management of Staff Representative Bodies (SRB)</b> | Workplace elections (electronic voting)   | Legal obligations                        |
|  | Management of SRB meetings  |  |
| <b>Litigation management</b>                           | Management of lawsuits (pre-litigation and legal disputes) with employees (or former employees, service providers or temporary employees)   | Legitimate interest                      |
| <b>Compensation and Payroll management</b>             | Payroll management and compensation tracking  | Contractual basis<br>Legal obligations   |
|  | Calculation and payment of deferred payments  | Contractual basis<br>Legal obligations   |
|  | Payroll management and declarations to compulsory and supplementary schemes (N4DS)  |  |
| <b>Organisation of working time</b>                    | Organisation of employee working time (absences, attendance time, working time calculation, working time tracking using badges)   | Contractual basis<br>Legitimate interest |
| <b>Disability management</b>                           | Management related to oversight of disability policies and compulsory declarations to the AGEFIP (DOETH)  | Legitimate interest<br>Legal obligations |
|  | Management of situations affecting the disabled (measures to help them to adapt and remain in the workforce)  |  |
| <b>Management of medical-social activities</b>         | Medical appointment tracking  | Contractual basis<br>Legal obligations   |
|  | Medical records and medical exam management   |  |
|  | Psycho-social risk management   |  |
|  | Management of cases dealt with by social workers  |  |

| Macro-purpose  | Sub-purpose   | Legal basis                              |
|--|---|--|
| <b>Recruitment<br/>Internal move</b>                         | Job application management (response to ads with CV and covering letter, responses to applications, publication of ads on the Natixis Intégrée and BPCE Group job sites, external publications)   | Legitimate interest                      |
|  | CV - CV library management  |  |
|  | Cooption management   |  |
| <b>Management of specific employee and pensioner schemes</b> | Management of payments  | Contractual basis<br>Legitimate interest |
| <b>Business travel and expense management</b>                | Booking of trips and reporting<br>Location of travellers<br>Trips by taxi and motorcycle taxi   | Legitimate interest                      |
| <b>General resource management</b>                           | Vehicle fleet management<br>Supplies and business card orders<br>Office supplies and equipment orders<br>Newspaper subscription management<br>Mail management<br>Tracking of requests made to the Real Estate and Logistics Department (DIL)<br>Management of moves and buildings<br>Photocopying | Legitimate interest                      |
| <b>Building security</b>                                     | Management of access control at the entrance and in identified areas<br>Security training management<br>Log books<br>Video surveillance   | Legitimate interest<br>Legal obligations |
| <b>BYOD CYOD</b>   | Provision of business mobile devices<br>BYOD/CYOD management  | Contractual                              |
| <b>Provision of computer hardware and software</b>           | Directories<br>Computer equipment management<br>Email<br>WiFi connection<br>Company social network  | Legitimate interest                      |
| <b>Monitoring of employees and cybersecurity</b>             | Control of computer hardware and software (software compliance, digital certificates)<br>Data collection and analysis<br>USB port blocking<br>Encrypted USB drives<br>Antivirus<br>Remote access to information systems (VPN)   | Legitimate interest                      |

| Macro-purpose                                 | Sub-purpose  | Legal basis          |
|---|--|----------------------|
| <b>Telephone management</b>                   | Incident management<br>Cost and duration management<br>Call routing<br>Voicemail<br>Directories  | Legitimate interest  |
| <b>Listening and recording</b>                | Listening to and recording telephone conversations and written messages (email and instant messaging) relating to trading room operations  | Legal obligations    |
| <b>Management of communication activities</b> | Management of internal contests and surveys<br>Invitation to events<br>Sending electronic greetings cards<br>Photo library management  | Legitimate interest  |
| <b>Fraud prevention</b>                       | Internal fraud prevention  | Legal obligations    |
| <b>Market abuse prevention</b>                | Price manipulation<br>Insider trading  | Legal obligations    |
| <b>Employee ethics</b>                        | Detection of conflicts of interest<br>Maintenance of lists of insiders and participants<br>Declaration of gifts, securities accounts, business cards, appointments and outside interests | Legal obligations    |
| <b>Whistleblowing</b>                         | Recording, investigation and processing of alerts  | Legal                |
| <b>Biometric access rights</b>                | Fingerprint authentication   | Consent              |
| <b>Audit and Inspections</b>                  | Risks controls and compliance monitoring   | Legitimate interests |

### How long will your Data be retained?

Most Data are kept for the duration of the contract of employment plus a specified number of years after the employee has left the company.

Our criteria for defining our retention periods are:

- Meeting our operational obligations in relation to human resources management (e.g. Data are kept 2 years for internal job applicants) and to secure our buildings and infrastructures (e.g. CCTV images are kept 1 month)
- Legal requirements (if any).

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

## 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.

In the above circumstances, **Natixis** may transfer your Data (by communicating or making it accessible) to the following recipients, based in France or in a 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:
  - o In relation to the sharing of resources, particularly financial and IT resources,
  - o In the event of restructuring involving a merger or similar transaction,
  - o In relation to internal move,
- IT providers (e.g. hosting, technical maintenance and support) and HR management related service providers (e.g. training providers, travel agents for business travels) in France and abroad,
- Bodies managing the various social insurance, unemployment insurance, retirement and provident schemes, paid holiday funds, public bodies and administrations legally entitled to receive them;
- Financial institutions involved in the management of NATIXIS' accounts and those of the employee,
- Staff representative bodies, trade union delegates, worker councils,
- Occupational medicine, social worker,
- Certain regulated professions (lawyers, notaries, auditors),
- The General Inspection departments of BPCE.

## **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:
  - o 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,
  - o 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:
  - o 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),
  - o 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?”

## 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**).

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.

## 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, contact details, your employer legal entity, and providing a copy of your identity document.

| <b>Data Protection Officer</b>               |  |
|--|--|
| Postal address                               | Email  |
| Natixis – BP 4 – 75060 Paris Cedex 02 France | <a href="mailto:dpo@natixis.com">dpo@natixis.com</a> |