NATIXIS
GLOBAL DATA PRIVACY POLICY

Version: v2

Date: 17/09/2020

CONFIDENTIAL

Natixis (or “we”, “our”) shall mean Natixis SA, a Joint-stock company established under French law, registered in Paris under no. 542 044 524 with a registered office: 30, avenue Pierre Mendès-France - 75013 Paris, France, and all of its worldwide subsidiaries and branches which are owned or controlled, directly or indirectly, by Natixis SA.

All capitalized terms not otherwise defined in the glossary is Policy have the meaning ascribed to them in the General Data Protection Regulation (GDPR).

1. INTRODUCTION

Privacy is about respecting individuals and safeguarding information pertaining to them.

Privacy is essential to creating an environment that fosters transparency and trust between organizations and individuals in the global and digital data economy.

We, at Natixis, are committed to meeting our obligations under applicable Data Privacy Law.

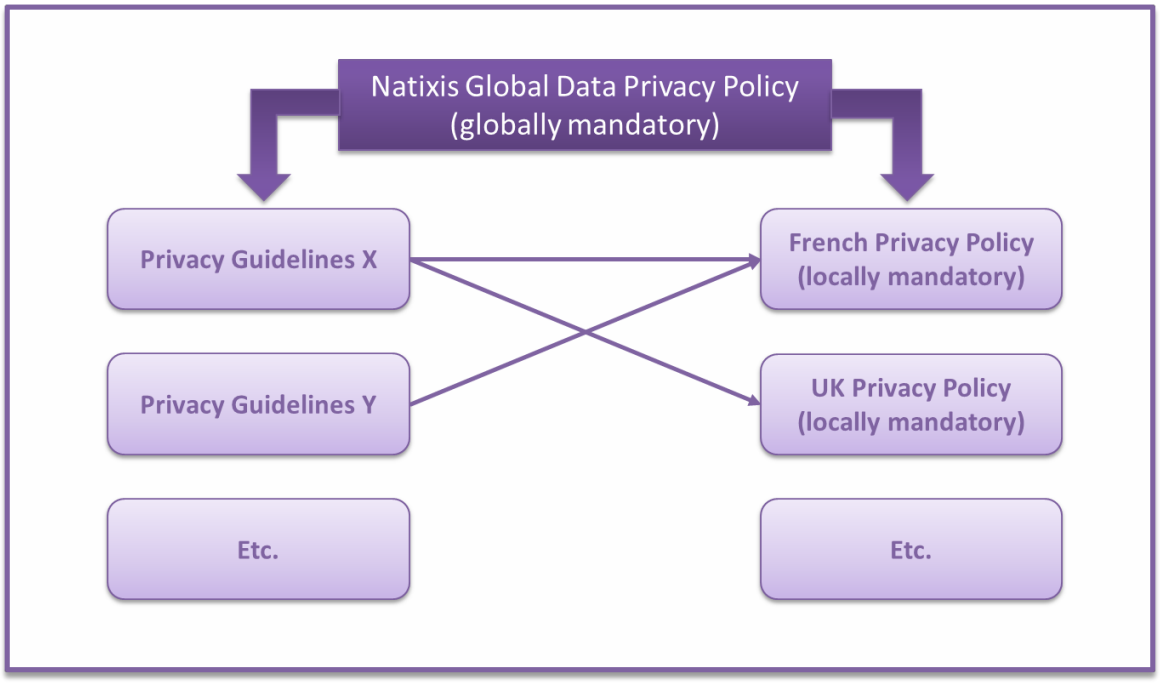
Non-compliance with Data Privacy Law can lead to very high sanctions, including severe revenue based fines, public warnings, temporary or definitive ban on data Processing and rights for individuals to claim compensation.

2. OBJECTIVE

Natixis Global Data Privacy Policy (this "Policy") describes the standards applicable to Natixis globally for the Processing of Personal Data.

In liaison with the Natixis DPO, Natixis local implantations issue their own national policy in compliance with this Policy.

Privacy Guidelines have been drafted to consider specific privacy topics (e.g. Privacy guidelines on consent or Data retention guidelines).



Local Privacy Procedures are locally available in English and local language(s).

3. SCOPE AND EXECUTION

3.1 Scope

This Policy applies to the Processing of all Personal Data (e.g. of employees, clients, suppliers, business partners) by Natixis or by a supplier acting/Processing on behalf of Natixis.

3.2 Compliance with this Policy

Natixis shall comply with this Policy, without prejudice to local legislation.

Applicable Data Privacy Law may require stricter standards or impose less stringent rules than those contained in this Policy. Therefore, Natixis may well adopt local privacy procedures that differ from this Policy subject to Natixis Data Protection Officer prior approval.

Besides,

- in case local laws and regulations are stricter, the local legislation and local policies (if any) will prevail;
- in case this Policy is stricter than the local legislation, this Policy will prevail, unless an exemption is granted by Natixis Data Protection Officer;
- in case this Policy would entail a breach of local legislation, it should be promptly reported to Natixis Data Protection Officer who will grant appropriate exemption.

Natixis DPO is recipient of any local privacy procedure.

3.3 Enforcement

Subject to local laws and regulations, Natixis will take appropriate remedial action, which may include disciplinary sanctions, if Personal Data are accessed, Processed or used in any way that is inconsistent with this Policy.

3.4 Publication

This Policy will be posted on Natixis intranet and may also be distributed (in hard or electronic version) as appropriate to employees.

Natixis employees involved in the Processing of Personal Data will be informed of the Policy's application.

4. GOVERNANCE AND RESOURCES

4.1 Natixis Data Protection Officer

Natixis has appointed a global corporate Data Protection Officer named "Natixis Data Protection Officer" or "Natixis DPO" with a statutory position defined by the GDPR.

To ensure the application of this Policy, Natixis Personal Data Protection Officer is responsible for:

- implement and interpret this Policy and report on it, in particular through an annual report on its activities to the Data Privacy Committee, the General Secretary and General Management;
- lead and drive:
    - the Data Privacy Community of the DPLs and local DPOs,
    - the Data Privacy Committee;

- define the normative framework of the Protection of Personal Data by:
    - Initiating and coordinating any necessary changes to this Policy and Guidelines,
    - establishing guidelines and internal rules for certain specific topics concerning the protection of Personal Data, and,
- in coordination with local DPOs and DPLs, inform and advise all Natixis entities and employees concerning their processing works and their obligations under this Policy and the applicable Personal Data Protection Legislation;
- control the compliance of the processing with this Policy and with the guidelines, the related policies and the Personal Data Protection Legislation, including:
    - by carrying out audits and establishing control plans applicable within Natixis entities,
    - consolidating the results of Level 2 permanent control and local risks mapping, and,
    - controlling the Personal Data Processing records of the controllers and the Categories of processing activities of the processors;
- initiating and carrying out training and awareness-raising activities for Natixis executives and employees on their obligations to comply with this Policy, the related policies and the Personal Data Protection Legislation;
- advice on any processing of Personal Data and in particular on:
    - the achievement and results of PIAs;
    - when a material risk persists in any data transfer;
- to receive, for its area of competence, directly or indirectly, requests from the Data Subjects and to ensure their treatment by the Controllers.

Natixis DPO is informed of all the complex requests of Data Subjects and is asked when security breaches occur on personal data.

Natixis DPO is entitled to give an opinion concerning any Personal Data Processing and in particular to request the Controller to modify the legal basis of one of its data processing.

Natixis DPO may also be a Local DPO for Natixis entities located in France and subject to this Policy.

4.2 Data Protection Community

4.2.1 Regional Data Privacy Liaison

Natixis appoints a Regional Data Privacy Liaison ("**Regional DPL**"), representing the Natixis DPO, who spearheads the community of Local DPOs and DPLs (Data Protection Liaisons) in a number of countries.

The appointment of the Regional DPL identifies the incumbent's geographic scope of powers.

The Regional DPL performs the functions of DPL Local for entities which do not have Local DPO or Local DPL within their competence area and, as such, to receive, for their area of competence, directly or indirectly, requests from the Data Subjects and to ensure their treatment by the Controllers.

Concerning those entities that do not have a Local DPO, the Regional DPL is also the main contact of the data protection supervisory authorities. He/she informs the Natixis DPO of any data protection supervisory authorities request. The Regional DPL is also responsible for the local implementation of the present Policy and for notifying the Data Subjects in the event of security breaches affecting their personal data.

The Regional DPLs perform level 2 controls in accordance with the control plan issued by the Natixis DPO.

The Regional DPLs report on their actions to the Natixis DPO.

4.2.2 Local Data Protection Officer

Local Data Protection Officers ("Local DPOs") are appointed within a Natixis entity, or for a country, when required by legislation on personal data protection, or when deemed necessary by the entity itself. They hold a statutory position legally allocated to them under the GDPR.

Without prejudice either to the specific missions entrusted to the Natixis DPO, or to the responsibilities and missions of the relevant Regional DPL, the following missions are assigned to the Local DPO:

- he/she sets up the national procedure in compliance with this Policy and the local legislation, by requesting, as the case may be, exemptions from the Natixis DPO and implements it;

- He/she cooperates with the personal data protection supervisory authorities empowered to control the entity in which he/she was appointed as Local DPO;

- He/she is the direct or indirect recipient of requests from Data Subjects, and ensures that they are handled by the Data Controllers within their scope.

- He/she ensures that a system to permanently control personal data protection within his/her Natixis entity(ies) is established, and performs level 2 controls on personal data protection affecting local activity;

- He/she is the primary contact for all audit or inspection controls, without prejudice to the statutory powers of the Natixis DPO;

- He/she provides the information required by the Data Office to keep the log of data processing activities;

- He/she gives advice, on request, concerning any impact analysis relating to data protection, and checks its execution;

- He/she helps to raise awareness, within the corresponding Natixis entity(ies), of personal data protection and compliance with the present Policy, and of the personal data protection legislation in force;

- He/she is the main contact within his/her Natixis entity(ies) for issues relating to personal data protection;

- He/she participates in investigation work in the event of any security weakness affecting personal data;

- Under the leadership of the Regional DPL to whom he/she reports, he/she actively participates in the Data Protection community;

- Except Natixis DPO written position, He/she is the main link between the Regional DPL and his/her corresponding Natixis entity(ies) for personal data protection issues, and, in this capacity:

    - Informs the relevant Regional DPL of any request made by the personal data protection supervisory authorities;

    - Keeps the relevant Regional DPL informed of any exchange with another Local DPO, or another DPL from an entity outside France or from a BPCE Group establishment;

    - Must report all difficulties encountered in terms of personal data protection, or any breach of the GDPR or legislation concerning personal data protection.

The Local DPO is authorized to give an opinion concerning any personal data processing within his/her scope of powers and, in particular, to ask the Data Controller to modify the legal basis of one of his/her processes.

The Natixis DPO may grant exemptions to Local DPOs concerning the performance of certain activities.

Local DPOs may also act on the instructions of the Regional DPL and the Natixis DPO. For the appointment of Local DPOs, the entities must ensure:

- the appointee's reachability (local language proficiency, geographic proximity and/or limited time difference);

- that there are no conflicts of interest with other activities;

- his/her legitimacy to conduct controls and risk management activities.

Any Local DPO appointment will be subject to the opinion of the Regional DPL and the Natixis DPO. The Local DPO is affiliated to the Natixis DPO by a strong functional link.

The names and professional contact details of Local DPOs are available on the Natixis intranet.

Each local Natixis entity must train its DPOs and provide them with the necessary resources to fulfil their mission. Moreover, the local Natixis entity must appoint a replacement for each Local DPO to ensure mission continuity.

4.2.3 Data Privacy Liaison

In the absence of any DPO appointment, a Data Privacy Liaison, or DPL, is appointed for each entity (subsidiary, branch or representative office) in countries in which Natixis is located, to ensure local management of personal data protection. When required, the DPL shall also bear the title determined by local regulations and perform the duties thereof. The DPL's organizational scope is identified and validated by the Natixis DPO.

Natixis entities may appoint more than one DPL. In this case, their scope of responsibility will be identified and specified to the Natixis DPO.

The DPL reports to the Department that appointed him/her, however, whenever possible, the DPL shall be an employee of the Compliance Division.

The Natixis DPO and Regional DPL are notified prior to any DPL appointment, and give an advisory opinion on the person designated for the position, in particular to avoid any conflict of interest when that person is to hold several functions.

Whenever possible, for the appointment of DPLs, the entities must ensure:

- the appointee's reachability (local language proficiency, geographic proximity and/or limited time difference);
- that there are no conflicts of interest with other activities;
- his/her legitimacy to conduct controls and risk management activities.

The Natixis entity must ensure the mission continuity of its DPL after consulting the competent Regional DPL.

The DPL works closely with the Natixis DPO or the relevant Regional DPL. He/she is the main link between the Natixis DPO or the relevant Regional DPL and his/her corresponding entity(ies) for personal data protection issues. However, the DPL is not the point of contact for personal data protection supervisory authorities; this is the role of the competent DPO, excepted if he/she is holding a complementary title as defined by the local applicable privacy regulations.

The DPL must coordinate with other players who contribute to the operational implementation of the national policy for personal data protection (Data Office, ISS-BC, Business Line Management, Support Function Management, etc.).

Each Natixis entity that appoints a DPL must ensure that incumbents are suitably trained in terms of personal data protection, and provide them with the resources needed to fulfil their missions.

As participants in data protection, DPLs:

- Are the Program Manager's main relays concerning data protection issues and, if applicable, contribute to the process to integrate privacy in projects (either local or the PSP one);
- Ensure the setup of the level 1 permanent control of personal data protection for any activity carried out in their Natixis entities; proceed with the level 2 controls at the request of the relevant Regional DPL;
- Provide the information required by the Data Office to keep the log of data processing activities;
- Are the primary contact for all audit or inspection controls, without prejudice to the statutory powers of the relevant Regional DPL and the Natixis DPO;
- May participate, either occasionally or regularly, in any body or committee whenever the corresponding agenda includes issues relating to personal data;

- Help to raise awareness of personal data protection, compliance with the Data Privacy law;

- Actively participate in the data protection community overseen by the Natixis DPO;

- Are the main link between the Natixis DPO and their entity for personal data protection issues, and, in this capacity:

    - Provide support for the work of their entity and of the relevant Regional DPL and the Natixis DPO if rights are exercised by a Person Concerned;

    - Perform the appropriate actions requested by the relevant Regional DPL and the Natixis DPO concerning their mission;

    - Notify the Natixis DPO of any request by the personal data protection supervisory authorities, and assist the DPO with exchanges and inspections in progress with these authorities.

    - Keep the relevant Regional DPL informed of any discussions with a Local DPO, or another DPL from an entity outside France or from a BPCE Group establishment;

    - Participate in investigation work, at the request of the Natixis DPO, in the event of any security weakness affecting personal data;

    - Voice their concerns or report breaches of legislation concerning personal data protection to the Natixis DPO or the relevant Regional DPL.

The DPLs concerned are informed of any data breach that falls within their scope of activity. The names and professional contact details of DPLs are available on the Natixis intranet.

The Regional DPL and the Natixis DPO are authorized to assign specific tasks, either occasionally or regularly, to the DPLs subject to prior notification of their associated entities, and provided such tasks are compatible with their main duties.

4.3 Natixis Data Privacy Committee

Natixis Data Privacy Committee is comprised of senior managers from all Business lines and organizational units and chaired by Natixis Data Protection Officer.

Its function is to cascade and promote Natixis Global Data Privacy Policy within Business lines and organizational units, discuss privacy topics as well as Natixis Data Protection Officer's reports and make related decisions where appropriate.

Natixis Data Privacy Committee will meet as often as Natixis DPO determines necessary and at least once a year.

5. DATA PROTECTION PRINCIPLES AND ACCOUNTABILITY

5.1 Principles

Although data privacy requirements vary throughout the world, they are based on globally accepted data protection principles stated in international regulations (OECD guidelines, UNO, Council of Europe, Apec framework).

Natixis will abide by the following principles when processing personal data:

5.1.1 Lawful Processing

Natixis needs to identify a legal basis (also referred to as the "conditions for Processing") before it can process personal data. It is important to determine our legal basis for processing personal data and document this.

Indeed, the legal basis for Processing has an effect on individuals' rights. For example, if Natixis relies on someone's consent to process their data, they will generally have stronger rights, for example to have their data deleted.

5.1.1.1 Conditions for Processing Personal Data

Natixis may process personal data if the processing falls within the scope of one of the following conditions:

a. Performance of a contract

The "contractual performance" permits the Processing of personal data in two different scenarios:

- Situations that take place prior to entering into a contract such as pre-contractual relations (provided that steps are taken at the request of the individual, rather than being initiated by Natixis):

  - *For example, if an individual requests information from Natixis about a particular product or service, the Processing of that individual's personal data is permitted for the purposes of responding to that enquiry.*

- Situations in which Processing is necessary for the performance of a contract to which the related individual is a party. This may include, for example:

  - *Processing identification data and bank details information for carrying out payment transfers and other financial transactions,*

  - *Processing employees' payroll, annual leave records and social benefits information.*

b. Compliance with legal obligations

This addresses cases where Natixis has a legal obligation to perform such Processing. This may include for instance:

  - *Compliance with tax regulations (Natixis as an employer may collect tax information of its employees),*

  - *Compliance with anti-money laundering and anti-terrorist financing regulations,*

  - *Mandatory call recording for banks and over-the-phone finance related activities.*

c. Legitimate interests

Natixis may Process Personal Data where it is necessary for its legitimate business' interests, unless such interests are overridden by the interests or fundamental rights and freedoms of the individuals concerned.

In case Natixis would rely on its legitimate interests for processing personal data, Natixis should record the assessment made to demonstrate that proper consideration has been given to the rights and freedoms of data subject.

Examples of Natixis' legitimate interests may be:

- *preventing fraud,*
- *internal management and management reporting, including but not limited to managing company assets, conducting internal audits and investigations,*
- *safety and security: activities involving safety and health, protecting Natixis assets, ensuring network and information security, including managing authentication and access rights, preventing unauthorized access to electronic communications networks and stopping damage to computer and electronic communication systems;*
- *protecting the integrity of Natixis, including: identification, prevention and investigation of activities such as breach of laws and regulations, criminal conduct,*
- *Natixis intra-companies transfer of employee/client data for internal administrative purposes.*

d. *Protecting the vital interests of individuals*

This is where Processing is necessary to protect the vital interests of an individual:

- *For example, urgent medical reasons.*

e. *Individual* consent

If Natixis cannot rely on one of the above previous conditions, or if applicable law so requires, Natixis shall only Process Personal Data with the individual's consent.

- Informed consent: consent must be 'informed' (i.e. the individual shall understand the risks associated with the Processing of their personal data before giving consent).

Therefore, the individual shall be made aware of:

- *the identity of the controller and the purposes for which the data will be processed;*
- any further information that is necessary to enable the data subject to understand the Processing to which they are being asked to consent (e.g. the nature of and categories of *personal d*ata, the categories of recipients to which the *personal data* are disclosed (if any), the existence and how individuals can exercise their rights, specifically to the right to withdraw consent at any time);

- Withdrawal or refusal of consent: Data subjects have the right to refuse to consent, and the right to withdraw any consent they have given.

5.1.1.2 Breach of laws and regulations other than privacy laws and regulations

If processing personal data involves committing a criminal offence, the Processing will obviously be unlawful. However, Processing may also be unlawful if it results in:

- a breach of a duty of confidence: such a duty may be stated, or it may be implied by the content of the information or because it was collected in circumstances where confidentiality is expected – medical or banking information, for example;

- a breach of an enforceable contractual agreement;

- a breach of industry-specific legislation or regulations.

5.1.1.3 Processing Sensitive Personal Data

Natixis shall process Sensitive Personal Data only to the extent necessary to serve applicable legitimate purposes and under one of the following conditions:

- the individual has given explicit consent to the Processing of those Sensitive Personal Data (except where applicable laws prohibit reliance on consent);

- the Processing is necessary for carrying out obligations of Natixis under employment, social security or social protection law, or a collective agreement;

- the Sensitive Personal Data have manifestly been made public by the individual;

- for the establishment, exercise or defense of legal claims;

- to protect a vital interest of an individual, but only where it is impossible to obtain the individual's consent first; or,

- as required by or allowed under applicable local law.

Subject to the conditions set forth above, Personal Data relating to criminal convictions and offences may be processed for protecting the interests of Natixis with respect to criminal offences that have been or, are suspected to be committed against Natixis, and for supporting the activities to safeguard and ensure the security and integrity of Natixis including (attempted) criminal or otherwise negative conduct.

Data concerning suspected persons may also be processed under applicable legal or regulatory conditions (e.g., whistleblower policy).

5.1.2 Purpose specification and limitation

Natixis shall collect and hold Personal Data for a purpose(s) that are specific and clearly stated.

Natixis shall make sure that it clearly and specifically identifies the business need(s) for which personal data are collected and held as well as be aware of the different sets of data kept and specific purpose of each.

Moreover, the data collected should only be processed in a manner compatible with that purpose(s):

- if the Data Subject would not expect the further use of the data, it is likely to be considered as 'incompatible use';

- processing personal data for secondary purposes may also be subject to additional privacy requirements (e.g. update of data Processing records, informing or getting consent of the related individuals).

Therefore, the relevant Data Protection Officer shall be consulted prior to any further / new processing of personal data.

5.1.3 Individual information requirements

5.1.3.1 Informed notice to individuals

In general, individuals should know the reasons why Natixis is collecting and retaining their data.

The information that individuals should receive may vary according to applicable laws but shall include at least:

- the main purposes for which their data are Processed;
- which Natixis company is responsible for the Processing;
- and other relevant information such as the categories of the Processed Data, the categories of recipients to which the personal data are disclosed (if any), what are the individuals' rights and how they be exercised.

The information must be provided in a concise, transparent, intelligible and easily accessible way, using clear and plain language.

Personal Data not obtained from individuals

Subject to Data Privacy Law, where Personal Data have not been obtained directly from the individual, Natixis shall request the provider to promptly cascade the informed notice to the individual as set out above.

Nevertheless, if the data collected are used to communicate with the individual, Natixis shall at the latest, deliver the above informed notice when the first communication takes place.

5.1.3.2 Derogations

Natixis does not have to deliver this information to the individual if it would be impossible or involve disproportionate effort. In these cases, the information notice must be made publicly available (e.g. via Natixis corporate privacy policy attached to websites).

Relevant Data Protection Officer shall make any decision in this regard.

5.1.4 Data Minimization

Personal Data must be adequate, relevant and limited to those which are necessary in relation to the purposes for which they are collected and/or further processed.

- the specific types of personal data that are collected for a particular purpose may vary, depending upon the reason for collection and applicable regulations;
- if Natixis receives Personal data that is not necessary or irrelevant for the intended purpose of collection, or beyond the scope of the information which was provided to the Data Subjects, Natixis shall take steps to prevent future excessive or irrelevant transmissions of personal data from the sender, and shall use reasonable means (such as destruction) to ensure that the irrelevant or excessive Personal data is not further processed.

- Data minimization shall apply to free text fields or documents as well as to any Transfer/data sharing of information.

5.1.5 Accuracy and up to date

Natixis shall take steps to ensure that the Personal Data it processes is accurate, and where necessary, corrected and kept up to date.

Personal Data which is inaccurate or incomplete, in regard to the purposes for which it was collected or for which it is further processed, shall, as appropriate, be erased or rectified.

5.1.6 Storage period

Natixis shall retain Personal Data consistent with legal and business retention requirements. In particular Natixis shall take reasonable steps to destroy the personal data when (i) it is no longer required for the purposes for which it was collected and/or (ii) the maximum retention period allowed by applicable law (if any) has elapsed.

5.1.7 Integrity and confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage and using appropriate technical and organizational measures.

State of art of technology, the cost of implementation and the sensitivity of information shall be taken into consideration for implementing security measures.

Personal Data Breaches are subject to a notification regime towards Data Protection Authorities (DPAs) and/or affected Data Subjects in most of countries. See section 6 “Personal Data Breach incidents”.

Any suspected or actual Personal Data breach (including loss of or damage to an equipment containing Personal Data) should be reported immediately after having become aware of it, to the relevant and Natixis Data Protection Officers and to the Information Security Officer

5.2 Accountability

Natixis is committed to meeting its obligations under applicable Data Privacy Law and shall take, on a global basis, a proactive, systematic and responsible attitude towards data protection compliance.

In order to demonstrate compliance with the principles set forth in this Policy, Natixis shall implement the following measures:

5.2.1 Records of Processing activities

Natixis shall maintain internal records of Processing activities involving personal data.

Natixis may be required to make these records available to the relevant Data Protection Authority for purposes of an investigation.

5.2.2 record of all categories of processing activities

As a personal data processor, Natixis shall maintain internal records of Processing activities involving personal data realized for the account of controllers.

Natixis may be required to make these records available to the relevant Data Protection Authority for purposes of an investigation.

5.2.3 Data protection by design and by default

Systems and technology implemented and used by Natixis shall be designed in such a way so as to ensure that by default: (i) data Processing is limited to what is necessary for the purposes for which the data was collected; and (ii) only those within an organization who need to access the personal data can do so.

That obligation applies to the amount of Personal Data collected, the extent of Processing, the period of their storage and their accessibility.

Restricting access to Personal Data, Data minimization, Pseudonymization and Anonymization are appropriate measures participating to demonstrate Data protection by design and Data protection by default:

- *Access (including 'read only') to Personal Data in systems/databases shall be based on users 'legitimate business needs'.*
- *Minimizing the collection and Processing of Personal Data to what is strictly necessary is a must (Data minimization).*
- *Pseudonymisation shall be considered whenever possible (When data has been pseudonymized it still retains a level of detail in the replaced data that should allow tracking back of the data to its original state).*
- *Anonymization goes a step beyond Pseudonymization (Data are considered anonymous if all identifying elements have been eliminated rendering a reverse compilation irreversibly impossible).*

5.2.4 Privacy impact assessments

Privacy impact assessments (or PIAs) are a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimizing or eliminating that impact.

PIAs will allow Natixis to determine appropriate measures to be implemented for compliance with applicable Data Privacy Law.

Natixis must carry out a PIA for specific Processing identified by Natixis DPO or when using new technologies and the Processing is likely to result in a substantial risk to the rights and freedoms of individuals.

Natixis shall seek the advice of relevant Natixis DPO on the carrying out of a PIA who will also monitor the performance of the PIA.

6. PERSONAL DATA BREACH INCIDENTS

Natixis SA implements a procedure for managing security vulnerabilities.

The procedure must be implemented at the level of all operators of information systems operated for Natixis. The relevant Information Security and Business Continuity management and the relevant DPO will appoint a Delegate in charge of investigations and who will coordinate any action related to a Data Violation incident.

The Crisis Staff will determine the notifications to be made to the Control Authority and the impacted data subjects, as applicable.

7. INDIVIDUAL RIGHTS INCLUDING INDIVIDUAL ACCESS REQUESTS

Subject to applicable Data Privacy Law and conditions, individuals have rights in respect of the Personal Data that Natixis hold about them: right to access, rectify, object and restrict the Processing of their Personal Data, right to erasure (or to be forgotten) and to data portability.

Relevant Data Protection Officer and Data Privacy liaison shall be identified as the recipients of any individual requests, and shall, upon reception, verify than the entire process (from acknowledgement of receipt up to responding & closing) is leading within 4 weeks unless stipulated otherwise in the Local Privacy Policy.

Natixis may object to requests that are obviously excessive, in particular by their number, or repetitive and systematic character.

8. PROCESSING REQUIRING SPECIFIC PROTECTION

8.1 Direct marketing

Direct marketing means the transmission of information to individuals, by Natixis or a supplier acting on its behalf, especially for commercial purposes (e.g. contacting individual by email, fax, phone, SMS, post or otherwise, to communicate information about a product or service).

In every communication that is made to the individual, the individual shall be offered the opportunity to opt-out of further direct marketing communication (opt-out). In such case, Natixis will stop sending further communication as requested by the individual.

If applicable law so requires, Natixis shall send to individuals unsolicited communication with the prior consent of the individual (opt-in).

Natixis shall keep records of individuals that used their opt-in or opt-out in order to manage appropriately direct marketing campaigns and communications.

8.2 Automated decision making (including Profiling)

Automated tools may be used by Natixis to make decisions about individuals but significant decisions (which produce legal or similarly significant effects concerning the individual) may not be based solely on the results provided by the automated tool, unless:

a) the use of automated tools is required or authorized by law;

b) the decision is made by Natixis for purposes of entering into or performing a contract, or

c) the individual has provided explicit consent.

However, suitable measures to protect the individual's rights and interests must still be in place.

For a), the law itself must contain suitable measures to safeguard the individual's interests. Profiling to ensure security and reliability of services or in connection with monitoring of fraud and tax evasion as types of automated decisions could be justified based on law.

For b) and c), at a minimum, this must include a right to obtain human intervention for the data subject to be able to express his or her point of view and to contest the decision; appropriate statistical techniques must be used; measures should be in place to correct inaccuracies and risks of errors; and security must be ensured and discriminatory effects prevented.

Automated decision-making based on racial or ethnic origin; political opinions, religious or philosophical beliefs, trade union membership; data concerning health or sex life and sexual orientation, genetic data, and biometric data where processed to uniquely identify a person, may only take place with explicit consent or where the processing is necessary for substantial public interest reasons and based on European Union or national law.

Profiling

Profiling is any form of automated Processing intended to evaluate certain personal aspects of an individual, in particular to analyze or predict their performance at work; economic situation; health; personal preferences; reliability; behavior; location; or movements.

When Processing personal data for profiling purposes, Natixis must:

- ensure that appropriate safeguards are in place (e.g. use appropriate mathematical or statistical procedures for the profiling);
- Implement appropriate technical and organizational measures to enable inaccuracies to be corrected and minimize the risk of errors.

8.3 Children's data

Children are vulnerable individuals deserving specific protection when Processing their Personal Data, specifically when using child data in marketing or for profiling purposes or in connection with the supply of services.

Informed notice addressed to children must be child-friendly and parental consent may be required in some cases, as per applicable Data Privacy Law.

8.4 Deceased person data

In relation with local specifics, in-house rules may frame data management related to deceased persons. These rules shall be implemented in applicable local privacy procedure.

9. DATA TRANSFERS

9.1 Transfers of Personal data

Transfers of Personal Data can occur within and outside group-affiliated companies, i.e. included among Natixis.

Any Transfer of Personal Data shall be based on a specific and legitimate business purpose, not breach the law (e.g. banking secrecy rules) and limited to what is necessary.

9.2 Transfers to Data Processors

Natixis shall enter into appropriate written contracts with suppliers to ensure that they Process Personal Data in accordance with this Policy, applicable Data Privacy Law and Natixis' instructions.

Data Processors shall have access to Personal Data solely for the purposes of performing the services specified in their applicable services agreements.

If Natixis concludes that a Data Processor is not complying with these obligations, it will promptly take appropriate actions.

9.3 Transfers to other Data Controllers

Natixis may need or be required to disclose certain Personal Data to other Data Controllers, within or outside Natixis. For example:

- *Natixis may share Personal Data with authorized users among its affiliates or branches especially for on boarding shared customers or conducting compliance activities across markets;*

- *Natixis may be required to disclose certain Personal Data to comply with applicable laws (e.g. disclosure of salary data or information to tax authorities).*

9.4 International Transfers:

Notwithstanding the above, most of Data Privacy Laws impose restrictions on the transfer of Personal Data abroad or to international organizations, in order to ensure that the level of protection of individuals afforded by their legislation is not undermined.

Before transferring Personal Data outside its country of origin, Natixis must ensure that recipients have adopted appropriate privacy and security controls to protect Personal Data, in accordance with applicable Data Privacy Law:

- *For instance, Natixis does not transfer Personal Data to Suppliers outside of the EEA unless, for instance, the EU Standard Contractual Clauses approved by the EU Commission are signed with the Supplier if the latter is located in a country which does not provide an adequate level of protection of Personal Data.*

10. NOTIFICATIONS TO DATA PROTECTION AUTHORITIES (DPAS) AND WORK COUNCILS

In some countries, the Processing of Personal Data is subject to notification to the local DPA so it can be registered and in some cases, a prior authorization may be necessary.

Besides, local Work Councils might be informed and/or consulted before a new data Processing project involving employees' information is implemented.

Privacy local policies shall identify the necessary steps.

11. TRAINING AND AUDITS

Natixis shall maintain programs to periodically monitor adherence to this Policy and to help ensure compliance of Natixis and employees with laws, requirements and contractual agreements that apply to the Personal Data processed.

Such programs shall include periodic training and audits that enable Natixis to verify that its Global Privacy Policy is accurate, comprehensive, prominently displayed, fully implemented and accessible.

12. NATIXIS POINT OF CONTACT

For any questions on this Policy please contact:

Natixis
Data Protection Officer
BP 4
75013 Paris
France

Email : *dpo@natixis.com*

13. APPLICATION DATE

This Policy shall apply from May 25th, 2018 and may be amended, at any time, by Natixis DPO.

APPENDIX 1
UK SUPPLEMENT TO THE GLOBAL DATA PRIVACY POLICY

This UK Supplement describes specific local data protection requirements under UK law, building on (and without prejudice to) the requirements for the Global Data Privacy Policy ("GDDP").

This is not an all-encompassing list of UK requirements – specific advice should be sought for specific scenarios.

1. Annual fee / registration obligation

Natixis must annually register and pay a fee to the UK data protection supervisory authority, the ICO.

Natixis's current registration (and next renewal date) can be consulted here: *https://ico.org.uk/ESDWebPages/Entry/Z8215785*

2. Additional offences

Both individuals and Natixis itself may be subject to prosecution for breach of certain additional offences created by the UK Data Protection Act 2018 ("UK DPA 2018"), in the event of the following:

1. Knowingly or recklessly:

    a. obtaining or disclosing personal data without the consent of Natixis or another relevant Controller;

    b. procuring the disclosure of personal data to another person without the consent of Natixis or another relevant Controller;

    c. after obtaining personal data, retaining it without the consent of the person who was the Controller in relation to the personal data when it was obtained; or

    d. selling data if it was obtained in circumstances in which an offence has been committed under (a)-(c)

    (UK DPA 2018, s170).

2. Knowingly or recklessly re-identifying information that is de-identified personal data without the consent of Natixis or another responsible Controller (UK DPA 2018, s171).

3. Altering, defacing, blocking, erasing, destroying or concealing information with the intention of preventing its disclosure pursuant to a subject access or portability request (UK DPA 2018, s173);

There are also offences relating to failure to comply with, or the taking of steps to frustrate, investigations or enforcement by the ICO, e.g. destroying documents after the ICO has issued the company with an "information notice" or an "assessment" notice.

3. Legal basis for processing Sensitive Personal Data

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.

The UK DPA 2018, Schedule 1 sets out extensive supplementary legal bases for processing Sensitive Personal Data and data concerning criminal offences or convictions.

3.1 Processing Sensitive Personal Data for employment or social security law purposes

Processing of Sensitive Personal Data necessary to perform or exercise obligations or rights conferred by law on Natixis or the data subject, under employment, social security or social protection law, is permitted, *provided* that the Controller puts in place an "appropriate policy document" ("APD"). (UK DPA 2018, Schedule 1, para. 1). An APD must:

a. explain Natixis's procedures for complying with the data protection principles laid out in GDPR Article 5;

b. explain Natixis's policies as regards the retention and erasure of personal data, including providing an indication of how long the personal data are likely to be retained; and

c. be retained for as long as the processing takes place (and then for six months when the relevant processing ceases), review it from time to time (if appropriate), and make the policy document available to the ICO without charge (if requested).

Natixis must additionally ensure that its record of processing activities (required by GDPR Article 30 and stored by Natixis on its Collibra IT portal) also:

1. includes which UK DPA 2018 Schedule 1 provision is being relied upon;

2. describes how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and

3. includes details on whether the personal data are retained and erased in accordance with Natixis' policies (and if not, it explains why not).

(UK DPA 2018, Schedule 1, paras. 38 – 41).

The discussion of an APD, and additional Record of Processing Activities contents, supplement section 5.2 of the main body of the Global Data Privacy Policy.

3.2 Processing Sensitive Personal Data for occupational health purposes, or pensions

Processing of Sensitive Personal Data for preventive or occupational medicine, the assessment of the working capacity of an employee, or other health or social care purposes, is lawful provided that it is done by or under the responsibility of a person committed to duties of secrecy as set out in GDPR Article 9(3). (UK DPA 2018, Schedule 1, para. 2; see also UK DPA 2018 section 11)

Processing Sensitive Personal Data for equal opportunities monitoring

Processing of certain Sensitive Personal Data for equal opportunities / anti-discrimination monitoring[1] is lawful, provided that:

a. the Controller has an APD and has supplemented its records as processing with necessary additional information (see 3.1 above);

b. only specified types of Sensitive Personal Data are used, for specified types of monitoring (e.g. only data concerning health can be monitored in order to ensure equal treatment and opportunities for people with different states of physical or mental health);

c. the processing must not be carried out for the purposes of measures or decisions with respect to a particular data subject;

d. the processing must not be likely to cause substantial damage or substantial distress to an individual; and

e. the legal basis does not apply if a data subject has notified the Controller of their objection to such processing, and the data subject gave the Controller a reasonable period of time in which to stop processing such data.

(UK DPA 2018, Schedule 1, para. 8)

Processing Sensitive Personal Data specifically for racial and ethnic diversity monitoring for senior hires

UK DPA 2018, Schedule 1, para. 9 sets out a legal basis for processing personal data revealing racial or ethnic origin, carried out as part of a process of identifying suitable individuals to hold senior positions in a company or other organisation (e.g. director, secretary or similar, or a senior manager, of a company), in order to ensure racial/ethnic diversity in senior leadership of that organisation, provided that:

a. Natixis has an APD and has supplemented its records as processing with necessary additional information (see 3.1 above);

b. Natixis cannot reasonably be expected to obtain the consent of the data subject, and is not aware of the data subject withholding consent; and

c. the processing must not be likely to cause substantial damage or substantial distress to an individual.

3.3 Processing Sensitive Personal Data to prevent or detect unlawful acts, dishonesty, failures in services, mismanagement, fraud, terrorist financing, money laundering, etc.

UK DPA 2018, Schedule 1, para. 10 sets out a legal basis for processing Sensitive Personal Data when the processing:

a. is necessary for the purposes of the prevention or detection of an unlawful act,

[1] Defined as "the purposes of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained."

b. must be carried out without the consent of the data subject so as not to prejudice those purposes, and

c. is necessary for reasons of substantial public interest.

Natixis must have an APD and must have supplemented its records as processing with necessary additional information (see 3.1 above), unless the processing (only) consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure.

UK DPA 2018, Schedule 1, paras. 11 and 12 contain related legal bases for processing Sensitive Personal Data without consent, as necessary for the substantial public interest in carrying out a function which is intended to protect members of the public against—

1. dishonesty, malpractice or other seriously improper conduct,

2. unfitness or incompetence,

3. mismanagement in the administration of a body or association, or

4. failures in services provided by a body or association.

(UK DPA 2018, Schedule 1, para. 11)

Where this is done in order to comply with, or assist another person to comply with, a regulatory requirement, UK DPA 2018, Schedule 1, para. 12 applies.

UK DPA 2018, Schedule 1, para. 14 sets out a legal basis for processing Sensitive Personal Data for fraud prevention purposes, and more specifically, where the processing consists of:

i. the disclosure of personal data by a person as a member of an anti-fraud organisation (as that term is defined in s. 68 of the UK Serious Crime Act 2007),

ii. the disclosure of personal data in accordance with arrangements made by an anti-fraud organisation, or

iii. the processing of personal data disclosed as described in sub-paragraph (i) or (ii).

UK DPA 2018, Schedule 1, para. 15 sets out a legal basis for processing Sensitive Personal Data to make disclosures necessary under UK anti-money-laundering ("AML") or UK law preventing financing of terrorist activities (section 21CA of the Terrorism Act 2000).

Natixis must have an APD and must have supplemented its records as processing with necessary additional information (see 3.1 above).

These provisions also provide a legal basis for processing personal data relating to criminal offences or convictions (UK DPA 2018, Schedule 1, para. 36).

4. Data subjects rights exemptions

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.

UK DPA 2018, Schedule 2 sets out extensive supplementary exemptions from data subject rights and related provisions (e.g. basic GDPR principles, such as storage limitation), for specific circumstances.

The precise conditions for such exemptions, and the GDPR provisions/rights that they cover, vary from case to case. Examples include:

4.1 Exemption to protect the rights of others

Compliance with data subject access requests does not extend to providing copies of information relating to another individual who can be identified from the information, *unless*:

a. the other individual has consented to the disclosure of the information to the data subject, or

b. it is reasonable to disclose the information to the data subject without the consent of the other individual.

UK DPA 2018, Schedule 2, para.16 further discusses matters to be considered when assessing whether it is reasonable to disclose the information to the data subject without the consent of the other individual.

4.2 Exemption from notice, *etc*., in case of likely prejudice to investigations and prosecutions, or to disclosures necessary for legal claims.

UK DPA 2018, Schedule 2, para. 2 provides an exemption to notice, access, erasure, correction and other data subject rights, in respect of internal or external investigations into suspected criminal matters, or to processing of personal data for the assessment or collection of a tax or duty or an imposition of a similar nature.

UK DPA 2018, Schedule 2, para. 5 provides an exemption to those same rights when disclosure of the data:

a. is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),

b. is necessary for the purpose of obtaining legal advice, or

c. is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

However, these exemptions only apply to the extent necessary to avoid “likely” prejudice to those purposes.

Certain rights are also set aside in respect of information that is covered by legal professional privilege (UK DPA 2018, Schedule 2, para. 19), or that might reveal the commission of an offence by Natixis (except for offences under the UK DPA 2018, perjury, or other UK laws against the making of false statements under law/oath).

Note that the provisions mentioned above apply to personal data processing generally, but that further rules and restrictions apply in respect of access to communications (e.g. recording live calls, monitoring incoming and outgoing Internet traffic and emails, accessing stored emails and voicemails, etc.). See, in particular, the *Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018*.

4.3 Exemptions for employment references

Several data subject rights do not apply to personal data consisting of a reference given (or to be given) in confidence for the purposes of—

a. the education, training or employment (or prospective education, training or employment) of the data subject,

b. the placement (or prospective placement) of the data subject as a volunteer,

c. the appointment (or prospective appointment) of the data subject to any office, or

d. the provision (or prospective provision) by the data subject of any service.

4.4 Exemptions in case of likely prejudice to markets/trading in regulated financial instruments

UK DPA 2018, Schedule 2, para. 21 provides an exemption to certain rights and related GDPR provisions in respect of personal data processed for the purposes of or in connection with a corporate finance service provided by certain regulated persons/firms (generally, in the financial services sector).

Subject to meeting several conditions in paragraph 21, the exemption applies if application of the relevant rights or provisions (i) would be likely to affect the price of certain regulated financial instruments, (ii) are reasonably expected to (for example) affect trading in that instrument, or business activity, and (iii) would have a prejudicial effect on the orderly functioning of financial markets or the efficient allocation of capital within the economy.

4.5 Exemption for likely prejudice to management forecasts, business activity, etc.

UK DPA 2018, Schedule 2, para. 22 provides an exemption to certain rights and related provisions in respect of personal data processed for the purposes of management forecasting or management planning in relation to a business or other activity, to the extent that the application of those provisions would be likely to prejudice the conduct of the business or activity concerned.

4.6 Exemption in case of likely prejudice to negotiations with the data subject

UK DPA 2018, Schedule 2, para. 23 provides an exemption to certain rights and related provisions in respect of personal data that consists of records of the intentions of Natixis in relation to any negotiations with the data subject, to the extent that the application of those provisions would be likely to prejudice those negotiations.

APPENDIX 2
GERMAN SUPPLEMENT TO THE GLOBAL DATA PRIVACY POLICY

This German Supplement describes specific local data protection requirements under German law, building on (and without prejudice to) the requirements for the Global Data Privacy Policy ("GDDP").

This is not an all-encompassing list of German requirements – specific advice should be sought for specific scenarios.

1. Criminal and additional administrative offences

Individuals (not Natixis as a legal entity but persons in charge of the processing activities) may be subject to prosecution for breach of certain criminal offences (punishable with imprisonment of up to two or three years or a fine) under the German Federal Data Protection Act ("FDPA"), in the event of the following:

1. Deliberately, with regard to non-publicly accessible personal data of a large number of people for commercial purposes:

    a. transferring the data to a third party, or

    b. otherwise making them accessible.

    (FDPA, Sec. 42 No. 1).

2. With regard to personal data which are not publicly accessible and in return for payment or with the intention of enriching oneself or someone else or harming someone:

    a. processing such personal data without authorisation, or

    b. fraudulently acquiring such personal data.

    (FDPA, Sec. 42 No. 2).

Both Natixis and individuals may be subject to prosecution for breach of an additional administrative offence related to consumer loan contracts or contracts concerning financial assistance for payment with a consumer (see Sec. 491 et seqq. of the German Civil Code) if, cumulatively:

a. the conclusion of these contracts is refused by Natixis,

b. the refusal is the result of information provided by a body that, for the purpose of transfer commercially collects, stores or modifies personal data to be used to evaluate the creditworthiness of consumers, and

c. Natixis did not immediately notify the consumer of this refusal and the information received from such body (except where this information would endanger public security or order).

The administrative offence may be punishable by a fine of up to fifty thousand euros.

(FDPA, Sec. 43 para 1 No. 2).

2. Legal basis for processing Sensitive Personal Data

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.

The FDPA (Sec. 22 para 1 No. 1) sets out supplementary legal bases for processing Sensitive Personal Data. Processing of Sensitive Personal Data by private entities is permitted where:

a. the processing is necessary to exercise the rights derived from the right of social security and social protection and to meet the related obligations,

b. the processing is necessary for the purposes of preventive medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services or pursuant to the data subject's contract with a health professional and if these data are processed by health professionals or other persons subject to the obligation of professional secrecy or under their supervision,

c. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; in addition to the measures referred to in subsection 2, in particular occupational and criminal law provisions to ensure professional secrecy shall be complied with.

(FDPA, Sec. 22 para 1 No. 1).

However, such processing is only lawful if safeguards are taken to protect such data. These safeguards must be tailored to the circumstances of the individual case and take into account the state of technological knowledge, costs of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. These *"suitable and specific"* safeguards may include technical and organisational measures, pseudonymisation, encryption, or the appointment of a Data Protection Officer (the FDPA lists overall 10 different examples, Sec. 22 para 2 FDPA).

3. Processing for new purposes

This section supplements section 5.1.2 of the main body of the Global Data Privacy Policy.

The FDPA (Sec. 24 para 1 FDPA) enables the alteration of the purpose for which personal data had originally been collected to the extent necessary:

a. for defence of national or public safety, or prosecution of criminal offences, and

b. to assert, exercise or defend civil claims (but only if the interest of the data subject does not prevail).

This also applies in the case of Sensitive Personal Data, but only if one of the exceptions of Article 9 para 2 of the GDPR or Sec. 22 FDPA (see under No. 2 above) were also met.

4. Data subjects rights exemptions

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.

The FDPA sets out supplementary exemptions from data subject rights for specific circumstances.

The precise conditions for such exemptions, and the GDPR provisions/rights that they cover, vary from case to case. Examples include:

4.1 Exemption from data subject access requests

Compliance with data subject access requests does not extend to providing copies of information:

a. if the data is processed for purposes of scientific or historical research, statistical purposes or archiving purposes in the public interest (Sec. 27 para 2, 28 para 2 FDPA),

b. if access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party (Sec. 29 para 1 s. 2 FDPA),

c. if providing information would interfere with the establishment, exercise or defence of legal claims (Sec. 34 para 1 No. 1 FDPA),

d. if processing includes data from contracts under private law and is intended to prevent harm from criminal offences (protection of e.g. fraud prevention files), unless the data subject has an overriding legitimate interest in receiving the information (Sec. 34 para 1 No. 1 FDPA), or

e. if the data were recorded only because they may not be erased due to legal requirements or only serve purposes of monitoring data protection or safeguarding data (e.g. backups) (Sec. 34 para 1 No. 2 FDPA). Data stored for the purpose of providing information to the data subject and preparing such provision may be processed only for this purpose and for purposes of data protection monitoring; processing for other purposes is generally only allowed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

4.2 Exemption from the requests for rectification, from restriction of the processing and from the right to object

If the data is processed for purposes of scientific or historical research, statistical purposes or archiving purposes in the public interest, the request for rectification, for restriction of the processing or to object to certain types of processing can be refused to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes (Sec 27 para 2, 28 para 2 FDPA).

4.3 Exemption from request for erasure

Section 35 FDPA provides for several exceptions of the obligation to erase data.

a. if data erasure would be impossible or involve a disproportionate effort due to the specific mode of storage and if the data subject’s interest in erasure can be regarded as minimal (Sec 35 para 1 FDPA).

b. if Natixis has reason to believe that erasure would adversely affect legitimate interests of the data subject or if erasure would conflict with retention periods set by statute or contract, the right for erasure may not apply (Sec 35 para 2 FDPA).

c. if erasure would conflict with retention periods set by statute or contract (Sec. 35 para 3 FDPA).

4.4 Exemption from request for data portability

The right to data portability shall not apply as far as this is likely to render impossible or seriously impair the achievement of the archiving purposes in the public interest, and this is necessary to fulfil those purposes (Sec. 28 para 4 FDPA).

Appendix 3
Italian Supplement to the Global Data Privacy Policy

This Italian Supplement describes specific local data protection requirements under Italian law, building on (and without prejudice to) the requirements for the Global Data Privacy Policy ("GDDP").

This is not an all-encompassing list of Italian requirements – specific advice should be sought for specific scenarios.

1. Additional offences

Individuals, including Natixis employees, officers and its management, may be subject to prosecution for breach of certain additional offences created by the Legislative Decree 196/2003 as amended by Legislative Decree 101/2018 ("Italian Privacy Code"), in the event of the following, provided that these events are not more severe offences:

1. Knowingly:

    a. processing traffic data or location personal data, or sending unsolicited marketing communications in breach of the relevant provisions (Italian Privacy Code, Articles 123, 126, 129 and 130), with the specific purpose to make its own or third parties' profit or to cause damage to the data subject (imprisonment between 6 months and 18 months);

    b. processing special categories of data or judicial data in breach of the relevant provisions (GDPR, Articles 9 and 10, and safeguards under Italian Privacy Code, Articles 2-sexies, 2-octies, 2-quatordecies), with the specific purpose to make its own or third parties' profit or to cause damage to the data subject (imprisonment between 1 year and 3 years); or

    c. transferring personal data in breach of the GDPR (Articles 45, 46, 49)

    (Italian Privacy Code, Article 167)

2. Knowingly disclosing or publishing automated files, or a substantial part of it, containing personal data subject to large-scale processing, with the specific purpose to make its own or third parties' profit or to cause damages to the data subject:

    a. in breach of the rules for processing data in the public interest, including special categories of data or criminal offences and convictions data (imprisonment between 1 year and 6 years); or

    b. without the consent of the data subject (imprisonment between 1 year and 6 years);

    (Italian Privacy Code, Article 167-bis)

3. Fraudulently obtaining an automated file, or a substantial part of it, containing personal data subject to large-scale processing, with the specific purpose to make its own or third parties' profit or to cause damages to the data subject (imprisonment between 1 year and 4 years);

    (Italian Privacy Code, Article 167-ter)

4. Releasing untruthful declarations or documents to the Italian Data Protection Authority is punishable by imprisonment of between 6 months and 3 years, or up to 1 year for those who interrupt or disturb official proceedings started by the Italian Data Protection Authority;

   (Italian Privacy Code, Article 168)

5. Failing to comply with any order of the Italian Data Protection Authority is punishable by imprisonment of between 3 months and 2 years;

   (Italian Privacy Code, Article 170)

6. Violating the provisions on remote controls and investigation of employees' opinions (as set out under Article 4 (1) and Article 8 of Law 300/1970) is deemed anti-union conduct (according to Article 38 of the law 300/1970).

2. Legal basis for processing Sensitive Personal Data

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.

Italian Privacy Code and specific measures issued by the Italian Data Protection Authority set out extensive supplementary legal bases for processing Sensitive Personal Data and data concerning criminal offences or convictions.

2.1 Processing Sensitive Personal Data for employment or social security law purposes

2.2 Processing of Sensitive Personal Data necessary to perform or exercise obligations or rights conferred by law on Natixis under employment or social security law is permitted (Article 2-sexies, paragraph 2 lett. dd) of the Italian Privacy Code) provided that it complies with the safeguards identified by the Italian Data Protection Authority (i.e. the processing is strictly relevant for the requirements for the processing of sensitive data in employment relationships – General Authorisation No. 1/2016 – i.e. Natixis may process sensitive personal data, in addition to the provisions of Art. 9 (2) GDPR, for the purposes of the recognition of benefits or the disbursement of contributions, the application of legislation on social security and assistance, including supplementary benefits, or on health and safety at work, as well as in tax and trade union matters, for the purposes of keeping accounts or the payment of wages, cheques, bonuses, other emoluments, donations or ancillary benefits, to guarantee equal opportunities in the workplace, to pursue specific and legitimate purposes identified by the statutes of associations, organisations, federations or confederations representing categories of employers or by collective agreements, with regard to trade union assistance to employers. *PLEASE NOTE that this authorisation is subject to replacement by specific safeguards to be released by the Italian Data Protection Authority likely in 2020*).

2.3 Processing Sensitive Personal Data for occupational health purposes, or pensions

Processing of Sensitive Personal Data for preventive or occupational medicine, the assessment of the working capacity of an employee, or other health or social care purposes, is lawful provided that it is done by or under the responsibility of a person committed to duties of secrecy as set out in GDPR Article 9(3).

Genetic data may not be processed for the purpose of establishing the professional competence of a job applicant, nor for the purpose of establishing the professional competence of an employee, even with the consent of the data subject (Article 1.4 of the

Requirements for the processing of special categories of data in employment relationships – General Authorisation No. 1/2016 – *PLEASE NOTE that this authorisation is subject to replacement by specific safeguards to be released by the Italian Data Protection Authority, likely in 2020*).

2.4 Processing Sensitive Personal Data for *i)* equal opportunities monitoring and *ii)* senior hires

Processing Sensitive Personal Data for *i)* equal opportunities monitoring and *ii)* senior hires is generally permitted (Article 2-sexies, paragraph 2 lett. dd) of the Italian Privacy Code). Nevertheless, please consider that, unlike provided by the law in other countries, in Italy Natixis is not allowed to collect Sensitive Personal Data (e.g. ethnic origin, disability, religion and sexual orientation) to actively ensure equal opportunities: the principle applicable in Italy is that the employer is not authorised to discriminate and for this purpose it cannot collect information that may be used to discriminate.

This does not apply, and Natixis is permitted to collect this kind of Personal Data only in those limited circumstances the law expressly requires it (e.g. obligation to employ a certain number of workers with disabilities).

2.5 Processing Sensitive Personal Data for racial ethnic diversity monitoring

Personal Data relating to diversity can be processed for the purposes of performance of a contract or to comply with laws.

Please note that, according to Article 8 of Statute of Workers (Law no. 300/1970), Personal Data can be processed only to assess working attitude (and racial and ethnic personal data fall out of this scope).

2.6 Processing Sensitive Personal Data for religious or philosophical beliefs, political opinions or trade union membership

During the course of the employment relationship, the employer or another person equivalent to him may process Personal Data such as religious or philosophical beliefs, political opinions or trade union membership only for the purpose of obtaining permits or limited to other cases provided for by law or collective agreements (Article 1.4.2 of the Requirements for the processing of special categories of data in employment relationships – General Authorisation No. 1/2016 - *PLEASE NOTE that this authorisation is subject to replacement by specific safeguards to be released by the Italian Data Protection Authority, likely in 2020* - and Article 2-sexies, paragraph 2 lett. dd) of the Italian Privacy Code).

2.7 Processing Sensitive Personal Data to prevent or detect unlawful acts, dishonesty, failures in services, mismanagement, fraud, terrorist financing, money laundering, etc.

Processing of Personal Data relating to the assessment of civil, disciplinary and accounting liability and for inspection activities is permitted (Article 2-*sexies*, paragraph 2 lett. dd) of the Italian Privacy Code).

Processing of Personal Data relating to criminal convictions and crimes or related security measures is permitted if authorised by a rule of law or, in the cases provided for by law, regulation, concerning, among others, the fulfilment of obligations and the exercise of rights by the owner or the person concerned in matters of labour law or otherwise within the framework of employment relationships, within the limits of established by-laws, regulations and collective agreements, in accordance with the provisions of Article 9(2), letter b), and Article 88 of the GDPR (Article 2-*octies* of the Italian Privacy Code).

3. Data subjects rights exemptions

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.

Italian Privacy Code introduces some restrictions on data subject rights and related provisions for specific circumstances:

3.1 Prevalence of other rights or interests as opposed to those of the GDPR (Articles 2-*undecies*, Italian Privacy Code)

All the rights listed in the GDPR (Articles 15-22) cannot be exercised by either filing a request to Natixis (or another data controller) or a complaint with the relevant data protection authority if this could result in actual and concrete damage to:

a) the interests protected under anti-money laundering laws and regulations;

b) interests protected under the provisions on support for victims of extortion claims;

c) parliamentary inquiry committee papers (Article 82, Italian Constitution);

d) activities carried out by a public body, other than public economic bodies, on the basis of an express statutory provision, for the exclusive purposes of monetary policy, the system of payments, the supervision of intermediaries and credit and financial markets, and the protection of their stability;

e) defensive investigations or the exercise of a right in court (this covers any kind of proceedings, including arbitrations and other alternative dispute resolutions mechanisms).

f) the confidentiality of the identity of the employee who reports the offence of which he has become aware in the course of his duties (Law no. 179/2017).

3.2 General restrictions to the notice and exercise of rights in case of investigations and prosecutions (Article 2-*undecies*, Italian Privacy Code)

The Italian Privacy Code provides that the notice to the data subjects about their processing, or the obligation to release a notice to the interested data subjects in case of a data breach, as well as the exercise of any of the data subjects rights is delayed, limited or excluded to safeguard the independence of the judiciary and judicial proceedings, provided that:

a. the data controller (Natixis) informs, without delay, the data subject(s) about this restriction, unless this notice could compromise the purpose of the limitation, and

b. to the extent and for the time that this is results being necessary and proportionate, Natixis takes into account the fundamental rights and legitimate interests of the data subject(s).

4. Rights concerning deceased persons

This section supplements section 8.4 of the main body of the Global Data Privacy Policy.

Italian Privacy Code has introduced into Article 2-*terdecies* some specifications to the rights of a deceased person.

In particular, according to this provision, the rights under Articles 15 to 22 of the GDPR relating to personal data concerning deceased persons may be exercised by those who have an interest of their own, or act to protect the person concerned, as their representative, or for family reasons worthy of protection. The willingness of the data subject to prohibit the exercise of these rights must be unambiguous and must be specific, free and informed, and the prohibition may concern the exercise of only some of these rights.

The exercise of the rights referred to in Articles 15 to 22 of the GDPR is not permitted in the cases provided for by law or when, limited to the direct offer of information society services, the data subject has expressly prohibited it in a written declaration submitted to the data controller or communicated to the latter.

5. General Obligations

While processing personal data, the processor shall act in accordance to the current privacy obligations.

In relation to that, the processor is authorized to perform[2]:

a) Collection;

b) Recording;

c) Organization;

d) Storage;

e) Consultation;

f) Disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction.

Moreover, full compliance with current privacy regulation requires that personal data shall be[3]:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization"); accurate and, where necessary, kept up to date, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ("accuracy");

d) kept in a form which permits identification of data for the period necessary to accomplish the purposes for which the personal data are processed, and no longer;

e) processed in a manner that ensures appropriate security of the personal data ("integrity and confidentiality").

[2] Art. 4, par. 2, Reg. 2016/679/EU
[3] Art. 5, Reg. 2016/679/EU

6. Operational Instructions on data processing and security

The current legislation on privacy requires that any processing of personal data should be lawful and compliant with the purposes of the processing; personal data should be kept up to date and complete.

In order to fulfil these obligations, the processor shall:

a) At the time when personal data are obtained, provide the data subject with all the information described by art. 13, Reg. 2016/679/EU;

b) When necessary, require and acquire data subject's consent;

c) Where personal data are collected from a data subject, check the personal data's accuracy;

d) Ensure data privacy and secrecy of all information which comes to knowledge for reasons of his/her activity.

7. Processing of personal data relating to criminal convictions and offences

Privacy Regulation requires that the processing of personal data relating to criminal convictions and offences shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law[4].

In particular, when recruiting new employees, the Firm can request employees' criminal records and charges (of a date not earlier than 90 days) in order to assess employee's professional skills[5].

When new employees are exposed to risks of corruption, the Firm can put in place, behind their consent, "background checks" aimed at verifying their past and preventing potential infringements.

8. Processing of personal data in case of job recruiting

When unsolicited applications are sent from potential candidates, information described by Art. 13 GDPR will be sent by the Firm to new candidates as soon as the latter comes into contact with them.

Processing of personal data contained in curricula does not require data subject's consent as long as the latter is involved and the processing is necessary for agreement's execution[6]. On the contrary, data subject's consent is due when processing special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data or data concerning health or natural person's sex life[7].

Data will be kept for 1 year.

[4] Art. 10, Reg. 679/2016/EU
[5] Art. 2-octies, Legislative Decree 196/2003
[6] Art. 111-bis, par. 2, Legislative Decree 196/2003
[7] Art. 9, par. 2, Reg.679/2016/EU

9. Use of Internet and the mailbox.

The firm allows the use of Internet and the mailbox by the employees. However, this service may be carried out only in accordance to the purposes of the Firm and only when it results necessary for the work's performance. It is strictly forbidden to use Internet for watching, listening to or spreading offensive or defamatory material. The mailbox's accounts belong to the Firm and all the correspondence shall not be considered private.

In this perspective, personal data shall be adequate, relevant and collected for explicit, specified and legitimate purposes.

The Compliance Manual and IT Policy give the Firm the right of checking Internet and mailbox access' in order to prevent potential abuses or misuses. Disciplinary sanctions are imposed for non-compliance regulation.

APPENDIX 4
SPANISH SUPPLEMENT TO THE GLOBAL DATA PRIVACY POLICY

This Spanish Supplement describes specific local data protection requirements under Spanish law, building on (and without prejudice to) the requirements for the Global Data Privacy Policy ("GDDP").

This is not an all-encompassing list of Spanish requirements – specific advice should be sought for specific scenarios.

1. Additional offences

There are additional offences created by the Organic Law 3/2018, of 5 December, on the Protection of Personal Data and granting the digital rights (the "**Spanish Data Protection Act**") in relation to specific local obligations and provisions. For example:

a. processing of criminal data when it is not permitted by law (please refer to section 2.2 for further information);

b. infringing the obligation of blocking personal data as required by law (please refer to section 4 below for further information in this regard); and

c. knowingly de-anonymising personal data in order to reidentify the data subjects affected.

There are also offences relating to failure to comply with, or the taking of steps to frustrate, investigations or enforcement by the Spanish Data Protection Authority (the "**AEPD**") or the activities carried out by the DPO.

2. Legal basis for processing Sensitive Personal Data

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.

2.1 Consent for processing certain special categories of personal data

Article 9(1) of the Spanish Data Protection Act states that the data subject's consent is not enough in order to process certain special categories of personal data concerning him (for example, ideology, trade union membership, religion, sexual orientation, beliefs or racial or ethnic origin) unless it is necessary for a clear and lawful purpose.

Said article states that *"when the main purpose* (of processing this data) *is merely identifying the ideology, trade union membership, sexual orientation, beliefs or racial or ethnic origin"* of the data subject, consent of the affected individual will not be enough to process this data.

The purpose of this provision is to avoid discriminatory situations (e.g. this prevents a company from not hiring an individual because of his/her racial origin).

2.2 Processing of criminal data

The processing of this kind of information is highly restricted in Spain in light of Article 10 of the Spanish Data Protection Act. This information can only be processed for the prevention, investigation, detection of potential criminal offences or in order to judge whether a criminal offence has been committed (i.e. the processing of this information is mostly restricted to competent authorities and law enforcement bodies) and by lawyers and barristers with the

purpose of providing a service to their clients. In any other case, this information can only be processed if it is provided by an applicable law.

3. Individual information requirements

This section supplements section 5.1.3.1 of the main body of the Global Data Privacy Policy.

Article 11 of the Spanish Data Protection Act enables controllers to provide information by means of a layered system (i.e. by providing the data subject with generic information on the processing of his/her personal data together with a link or reference to a document that contains the full set of information that needs to be provided in light of Articles 13 or 14 of the GDPR).

The first layer of information should include, at least, the following information:

a. The identity of the controller (already included in the heading of the contract); and his representative

b. The purposes of the processing; and

c. The possibility to exercise certain rights between the articles 15 to 22 of Regulation EU 2016/679 of the European Parliament.

If the information was not directly gathered from the data subject, further to the above, information on the source from which the personal data were collected and the relevant categories of personal data also needs to be provided.

4. Obligation to block data

This section supplements section 5.1.6 of the main body of the Global Data Privacy Policy.

The Spanish Data Protection Act states in its Article 32 that when personal data needs to be erased (either because it is no longer necessary for the purposes for which it was collected or either as a consequence of a data subject's request) the personal data shall be kept duly blocked for an additional period of time for the exercise or defence of legal claims. By duly blocked, the Spanish Data Protection Act means storing the information in a way that the personal data is not accessible by anyone in a company unless it is requested by competent public administrations or for the exercise or defence of legal claims. Blocked data cannot be processed for any purpose other than those indicated above. Once the blocking period elapses, the personal data can be fully destroyed.

5. Marketing

This section supplements section 8.1 of the main body of the Global Data Privacy Policy.

In light of Article 21 of Law 34/2002, of 11 July, on Information Society Services and e-Commerce (the "**ISS Act**") consent is necessary in order to send marketing communications through electronic means (both B2C and B2B).

Consent could be waived however (i.e. a soft opt-in solution could valid) if the following requirements are met: (i) there is already a contract between the sender and the recipient; (ii) the data have been lawfully collected; (iii) the potential recipient has been offered the possibility to object to receiving market communications, at the point his/her data were collected and is offered the possibility to object within each communication; and (iv) the communications relate to products and/or services of the sender itself, directly related to the ones that constituted the subject matter of the existing contract between both parties.

Further to this, if the marketing activity entails the processing of personal data, in light of Article 23 of the Spanish Data Protection Act, addresses must be screened against marketing blacklists recognised by the Spanish Data Protection Authority. Currently there is only one: Lista Robinson https://www.listarobinson.es/.

6. Children's data

This section supplements section 8.3 of the main body of the Global Data Privacy Policy.

Children's consent will only be lawful if the minor is over fourteen years old. In any other case, the child's legal representative's consent shall be necessary.

7. Deceased persons' data

This section supplements section 5.1.3.1 of the main body of the Global Data Privacy Policy.

The next of kin of a deceased personal have the right to request access to the personal data concerning the deceased person, as well as the right to rectification and erasure (unless the deceased person stated otherwise or it is forbidden by law). These rights can also be exercised by the individuals/entities specifically appointed by the deceased person.

APPENDIX 5 RUSSIA SUPPLEMENT TO THE GLOBAL DATA PRIVACY POLICY

This Russia Supplement describes specific local data protection requirements under Russian law.

This is not an all-encompassing list of Russian requirements – specific advice should be sought for specific scenarios.

For the purpose of this Appendix 5, Natixis (or “we”, “our”) shall mean Natixis Bank JSC, Moscow.

1. Data Protection Officer

The Federal Law No 152-FZ dated 27 July 2006 On Personal Data (the "**PD Law**") requires Natixis to appoint a Data Protection Officer (the "DPO"). The DPO is appointed by and is accountable to Natixis' executive body.

The PD Law imposes the following key duties on the DPO:

1.1 to carry out internal audits over compliance of Natixis and the Natixis' staff with the Russian legislation requirements for personal data, including requirements on the protection of personal data;

1.2 to arrange communications to Natixis staff on relevant provisions of the Russian legislation on personal data, internal regulations on processing of personal data and the requirements to protect personal data; and

1.3 to implement policies for receipt and handling of the data subject requests or their representatives and/or control of the receipt and handling of such applications and requests.

2. Data Protection Principles

2.1 Natixis will abide by the following principles when processing personal data:

2.1.1 lawful and fair processing of personal data;

2.1.2 only processing personal data that meets specific, defined and legitimate purposes of processing. Natixis is prohibited to process personal data which is incompatible with the purposes for which personal data was collected;

2.1.3 ensuring that the content and scope of personal data processed match the purposes of processing and personal data processing is not excessive in relation to the purposes of processing;

2.1.4 not combining databases containing personal data processed for purposes which are not compatible with one another;

2.1.5 ensuring that personal data processed is accurate, sufficient and relevant in relation to the purposes of processing; ensuring measures are taken for removing or updating inaccurate or incomplete data;

2.1.6 storing personal data in a way that allows identification of a data subject; it should be for no longer than required by the purpose of processing, except where the data retention period is provided by the federal laws or a contract to which the data subject is a party, of which the data subject is a beneficiary or guarantor;

2.1.7 procuring that personal data is destroyed or anonymised upon the achievement of the purposes of processing or in case processing the personal data is no longer needed, except where otherwise provided by the federal laws.

3. Lawful processing

3.1 Natixis shall ensure that any processing of personal data is carried out on the basis of legitimate grounds for processing of personal data which are listed exhaustively in the PD Law and include, among others:

3.1.1 performing an agreement, including an employment agreement, of which the data subject is: a guarantor or beneficiary; or entering into an agreement at the initiative of the data subject;

3.1.2 consent of the data subject;

3.1.3 where processing is required to achieve the purposes of an international agreement to which Russian Federation is a party or of a federal law, or to discharge and comply with the functions, rights and obligations of a data operator which are provided in the Russian legislation (for example, processing of the employees' data and providing such data to the tax authorities, social security funds (pension funds, etc.));

3.1.4 processing of personal data in the public domain to which the data subject gave access to an unlimited number of people or such access was given at the data subject's request;

3.1.5 legitimate interests of the data operator, subject to the rights and freedoms of the data subject not being affected. Although legitimate interest is one of the statutory legitimate grounds for processing of personal data, it is rarely relied on due to lack of enforcement practice and lack of clarity on the requirements that legitimate interest should not breach rights and freedoms of a data subject.

4. Consent of data subject

4.1 Consent should be specific, informed and conscious. The Russian DPA has clarified that:

4.1.1 the consent is specific if it is explicitly expressed, substantive, definitive and not vague;

4.1.2 the consent is informed if it represents a notifying and communicating intention which confirms the respective event, fact and/or action;

4.1.3 the consent is conscious if it is meaningful, deliberate and reasonable.

4.2 Unless the written consent is required by the federal laws, consent to processing of personal data may be granted in any form which allows Natixis as the data operator to

prove that the consent is obtained. The burden of proof that the consent for the processing of personal data was obtained lies with the data operator.

4.3 Written consent is required, among others, for:

4.3.1 processing of personal data of employees (consent for transfer of personal data to third parties, for disclosure of personal data for commercial purposes, for obtaining the employee's personal data from a third party as further provided in section 10 below);

4.3.2 including personal data in public data resources;

4.3.3 processing of sensitive personal data which under Russian law is referred to as special categories of personal data, which is data on racial/ethnic origin, political opinions, religious/philosophical beliefs, state of health (in the employment context the latter should be restricted to information which relates to the employee's ability to perform the job as further provided in section 10.4.4) and sex life;

4.3.4 processing of biometric personal data;

4.3.5 cross-border transfers and processing of personal data in the countries which do not provide an adequate protection of the rights of the data subjects and where there is no other ground justifying the transfer, for example, to perform a contract to which a data subject is a party; and

4.3.6 the data operator is entitled to pass a decision on the basis of exclusively automatic processing of personal data if such decision results in legal consequences in relation to the data subject or in any other way affects the data subject's rights and legitimate interests (such way of passing a decision is expressly prohibited in relation to the employees).

4.4 A written consent shall include:

4.4.1 full name of the data subject, details of the identification document (number, date of issue and an authority which issued the document) (if the data subject is represented by his representative, the same information should be provided in relation to the representative). In the majority of cases a passport is the ID;

4.4.2 name of the data operator and its registered address;

4.4.3 purpose of processing;

4.4.4 the scope of personal data to the processing of which the data subject granted his/her consent;

4.4.5 name and registered address of the personal data processor (if any) who is authorised by the operator to process personal data;

4.4.6 scope of data processing operations and specific ways of processing (automated/non-automated) authorised by the consent;

4.4.7 time period within which the consent is valid and the procedure to revoke the consent; and

4.4.8 data subject's signature.

4.5 The consent in the form of an e-document which is signed by the e-signature in accordance with the federal laws is deemed to be equal to the consent granted in hard copy. The Russian DPA informally commented that, where prior written consent to processing of personal data is required, a simple e-signature should be sufficient. Having said that, based on the strict interpretation of the Russian legislation, written consent provided as an electronic document should be signed by an enhanced encrypted and certified e-signature.

4.6 The data subject may revoke the consent at any time. If the consent is revoked by the data subject, Natixis as the data operator may continue processing personal data without the consent in cases prescribed by the PD Law.

5. Individual rights including individual access rights

5.1 Except where providing the data subject with access to his/her personal data violates the rights and legitimate interests of the third parties and in other cases provided for in the federal laws, the data subject has the right to request information from the data operator regarding processing of personal data which includes, but is not limited to:

5.1.1 confirmation of the fact that the data operator is processing their personal data;

5.1.2 legal grounds and purposes of the processing of personal data;

5.1.3 purposes and methods of processing of personal data used by the data operator;

5.1.4 name and location of the data operator, information about persons (except for employees of the data operator), who have access to personal data or to whom personal data may be disclosed under a contract with the data operator or on the basis of a federal law;

5.1.5 scope of personal data processed which relates to the relevant data subject and the sources from which the relevant data has been obtained (unless another procedure for providing such data is set out by a federal law);

5.1.6 timing for processing of personal data including retention periods;

5.1.7 the procedure on how the data subject can exercise his/her right under the PD Law;

5.1.8 information on cross-border transfers of data which have been or are planned to be carried out;

5.1.9 name of a company and/or the full name of an individual and their address which process personal data under a contract with the data operator if processing is or is going to be outsourced to the said persons;

5.1.10 other information prescribed by the PD Law and/or other federal laws.

5.2 The data subject has the right to require the data operator to correct his/her personal data, to block or destroy personal data in case personal data is incomplete, outdated, inaccurate, unlawfully obtained or is not necessary for the stated purpose of processing, and to take legal action to protect his/her rights.

5.3 The data subject has the right to withdraw consent previously granted and require a termination of processing of his/her personal data.

5.3.1 If the data subject considers that the data operator carries out processing of personal data in violation of the PD Law or otherwise violates his/her rights and freedoms, the data subject may appeal the acts or omissions of the data operator to the DPA or in court.

5.3.2 The data subject has the right to defend his/her rights and legitimate interests, including the protection of his/her personal and family secrets, including the right to be compensated for damages and/or moral harm in court, and appoint for these purposes his/her representatives.

5.4 In addition to the rights provided above, the data operator's employee may also:

5.4.1 complement the personal data which provides an evaluation by a statement expressing his/her own point of view;

5.4.2 has free of charge unrestricted access to his/her personal data, including the right to receive copies of any record containing personal data.

6. Data transfers

6.1 Data processing agreement

6.1.1 Natixis shall enter into a data processing agreement with any third party to whom Natixis outsources personal data processing which shall specify:

6.1.1.1 the particular personal data processing operations the processor is authorised to carry out;

6.1.1.2 the purpose of the processing;

6.1.1.3 the processor's obligation to keep the personal data confidential and secure the protection of the personal data whilst processing the data;

6.1.1.4 the requirements for specific legal, technical and organisational measures pursuant to the PD Law in regard to the personal data processed;

6.1.1.5 in relation to the employee data only, data operator should request confirmation from the processor that the employee data is only used for the disclosed purposes (please see further section 6.1.1.5).

6.1.2 The PD Law does not require indicating the scope of personal data which is subject to the data processing agreement but the views emerging from the DPA suggest that it is prudent to include the scope of personal data.

7. International transfers

7.1 Transferring personal data to countries which are the member-states of the European Council Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the "**Convention**") is subject to prior consent of a data subject in any form. The same rules apply to the countries which according to the

DPA's public list are not the member-states of the Convention but provide the adequate protection of the data subjects' rights. The list is currently comprised of 22 countries including, among others, Australia, Canada, Singapore, Japan and Israel.

7.2 In case of the cross-border transfer of personal data to the countries which do not provide the adequate protection of the data subjects' rights including, but not limited to, the USA, the data operator shall seek written consent from the data subject except where such trans-border transfer may be justified otherwise, for example, by performing a contract to which a data subject is a party.

7.3 Cross-border transfers of employees' personal data is always subject to the prior written consent of the employees as such transfer amounts to disclosure of data to a third party (please see further section 10.3.1 below).

8. Notification to DPA

8.1 Except where exemptions apply, the data operator is required to notify the DPA about its intention to process personal data prior to commencing processing. We note that Natixis has filed a DPA Notification, the information of which is available in the Russian language in the public register of data operators.

8.2 Once filed, the notification needs to be maintained and the DPA needs to be notified of any changes in the notification and/or ceasing the processing of personal data within ten (10) business days from such changes and/or ceasing of processing.

9. High level review of technical and organisational measures

Natixis as the data operator is entitled at its discretion to determine the scope of the measures which are required for and sufficient to complying with the duties imposed on the data operator by the DP Law. However, the data operator is required to undertake at least the following measures indicated in the DP Law:

9.1 appointing the DPO (please see section 1 above);

9.2 producing a set of internal regulations which clarify the data operator's policies in regard to processing of personal data, procedures for preventing and discovering of infringements of Russian legislation and eliminating the consequences of such infringements. Russian data protection legislation does not provide for an exhaustive list of documents which should be issued by the data operator;

9.3 implementing the legal, organisational and technical measures to ensure the security of personal data:

such measures, among others, include (i) determining the level of threats to the security of personal data while processing relevant data; (ii) determining the scope of the organisational and technical measures which match the levels of protection set out by the legislation; (iii) assessing the effectiveness of the measures implemented; (iv) keeping a record of the computers and other similar means of processing personal data; (v) detecting unauthorised access to personal data, establishing the facts and taking respective actions; and (vi) setting the rules for access rights to personal data and arranging recording of all actions with personal data;

9.4 implementing the measures of internal control and audit;

9.5 assessment of harm which may be caused to the data subjects in case of any unauthorised actions and whether the measures implemented by the data operator for compliance are sufficient for obligations imposed by the legislation;

9.6 familiarising the data operator's staff who process personal data with data protection legislation and the data operator's data protection policy and/or arranging for the staff training;

9.7 ensuring that all employees (rather than only the employees who process personal data) have read, understood and acknowledged in writing the data operator's policy on processing personal data and given their written consent to transfer of personal data to third parties including to affiliates and trans-border transfer (if any) (please see further section 10.2 below).

10. Processing of employees' personal data

10.1 Purposes of processing

The legitimate purposes of processing of employees' personal data are determined by the Russian Labour Code and include:

(a) compliance with legislation;

(b) assistance in gaining employment, obtaining education and job advancement;

(c) providing personal security to employees; and

(d) quantity and quality control in relation to the work done and protection of property.

10.2 Internal regulations on personal data

10.2.1 Natixis is required to produce a set of internal regulations on personal data protection including the procedures for processing personal data, circulating personal data within Natixis and the employees' rights and obligations in relation to processing personal data. All employees, including their representatives (if any), should read, understand and acknowledge in writing the internal regulations issued by Natixis.

10.2.2 Natixis is also required to approve a list of designated persons who are authorised to process personal data and ensure that only these individuals have access to personal data and strictly within the scope which is required for the purposes of work they are assigned to do. Any transfer of the employees' personal data within Natixis should be subject to internal regulations.

10.3 Disclosure of employees' personal data to third parties

10.3.1 Unless otherwise provided for by federal laws, Natixis is allowed to transfer employee's personal data to a third party including transfer for any commercial purposes subject to the employee's prior written consent (please see section 4 above).

10.3.2 Natixis shall warn the third parties receiving employee's personal data that this data shall be used in compliance with the confidentiality regime only for

the purposes for which it is transferred and require those third parties to confirm that this is complied with.

10.3.3 Natixis should provide personal data to the employee's representatives in the manner prescribed by federal laws and limit information only to the employee's personal data which is necessary to perform the functions of his/her representatives.

10.4 Personal data which an employer may process

10.4.1 Generally, Natixis is required to determine the scope of an employee's personal data to be processed in accordance with the Russian Labour Code, PD Law and other legislation.

10.4.2 Natixis shall receive the personal data of the employees from the employees themselves. If the employee's personal data can be obtained only from a third party, Natixis shall notify the employee and obtain the prior written consent for collecting of personal data from the third party. To obtain the employee's consent, Natixis shall inform the employee of the purposes, sources and methods of obtaining personal data, the nature of personal data and consequences of failure to get written consent by the employee to request such personal data. In requesting personal data, Natixis shall appreciate that the employees have their rights to preserve and can protect their confidentiality.

10.4.3 Natixis is prohibited from requesting and processing personal data about the employee's membership in public associations or trade union activities except where authorised by the federal laws.

10.4.4 Natixis is allowed to ask the employee to provide the sensitive personal data (special categories of personal data) only in cases established by federal laws. Information about the employee's health may only be requested in cases where such information is relevant to the ability of the employee to perform the work attributable to his/her role.

11. Localisation requirements

11.1 The PD Law envisages the following data localisation requirements:

11.1.1 When collecting personal data, including on the internet, Natixis is obliged to ensure that the personal data of the Russian citizens is recorded, systemised, accumulated, stored, updated (renewed and modified) and retrieved by using the data bases stored on servers which are situated in Russia, subject to the certain exceptions of the PD Law.

11.1.2 The scope of the data processing operations covered by the PD Law does not include using, transferring (disseminating, providing, accessing), anonymising, blocking, deleting and destroying personal data. The latter data processing operations are not covered by the data localisation.

11.2 Subject to compliance with the general rules on trans-border transfer of data (see further section 7 above), personal data of the Russian citizens which is initially entered into and modified in a database in Russia ("primary database") may be transferred to a database abroad which is administered by another Natixis group company ("secondary database").

APPENDIX 6

UAE SUPPLEMENT TO THE GLOBAL DATA PRIVACY POLICY

At the time of writing, there is no Federal Data Privacy Law in the UAE. An individual right to privacy is enshrined in the UAE Constitution and the Penal Code. More comprehensive data protection laws apply to companies incorporated in a free zone with its own data protection laws, such as the Dubai International Finance Centre (DIFC).

Since Natixis SA has a branch in the DIFC, this UAE Supplement describes specific local data protection requirements under the *DIFC Data Protection Law 2020 (DIFC Law No. 5 of 2020)(the "Data Protection Law") and the DIFC Data Protection Regulations (the "Regulations")*, building on (and without prejudice to) the requirements for the Global Data Privacy Policy ("GDDP").

This is not an all-encompassing list of UAE requirements – specific advice should be sought for specific scenarios.

1. Annual fee / registration obligation

1.1 Fees:

Natixis should have submitted a data protection notification and paid an initial registration fee of USD 1,250 for entities regulated by the DFSA when it was first incorporated in the DIFC (Registration). The data protection notification renewal is part of the license renewal request and an annual registration fee of USD 500 to the Commissioner of Data Protection at the DIFC will apply. A table of fees can be found at App1 of the Regulations.

Natixis can access information related to its registration by signing in to the DIFC Client Portal: https://portal.difc.ae/clientportal/s/login/

1.2 **Offences**:

Natixis may be subject to a fine if it is found to have contravened a provision of the Data Protection Law (the "Law"). The fines for each contravention are set out below and in Schedule 2 of the Data Protection Law.

Article	Contravention	Maximum Fine (USD)
9	Failing to comply with general requirements specified under Article 9 of the Law made for the purpose of this Law	$50,000
10	Failure to comply with requirements for lawful Processing specified under Article 10 of the Law made for the purpose of this Law	$50,000
11	Failure to comply with requirements for obtaining consent specified under Article 11 of the Law made for the purpose of this Law	$50,000
12	Failure to comply with requirements for lawful Processing specified under Article 12 of the Law made for the purpose of this Law	$50,000
14(1)	Failure to comply with the requirements for accountability specified under Article 14(1) of the Law made for the purpose of this Law	$25,000
14(2)	Failing to implement and maintain technical and organisational measures to protect Personal Data in accordance with Articles 14(2) of the Law made for the purpose of this Law	$50,000
14(3)	Failure to comply with the requirements for accountability specified under Article 14(3) of the Law made for the purpose of this Law	$25,000
14(4)	Failure to comply with the requirements for accountability specified under Article 14(4) of the Law made for the purpose of this Law	$25,000
14(5)	Failure to comply with the requirements for accountability specified under Article 14(5) of the Law made for the purpose of this Law	$25,000
14(7)	Failing to register with the Commissioner in accordance with Article 14(7)	$25,000
15	Failing to maintain records of any Personal Data Processing operations in accordance with Article 15	$25,000
16	Failing to appoint a DPO in accordance with Articles 16(2) and 16(3) of the Law made for the purpose of this Law	$50,000
20	Failing to carry out a data protection impact assessment prior High-Risk Processing Activities in accordance with Article 20 of the Law made for the purposes of this Law.	$20,000
22	Failing to comply with the requirements specified under Article 22(1), 22(2), 22(5) or 22(6) of the Law made for the purpose of this Law	$25,000
23	Failing to comply with the requirements specified under Article 23 of the Law made for the purpose of this Law	$25,000
24	Failing to comply with the requirements specified under Article 24(1), 24(3) or 24(6) of the Law made for the purpose of this Law	$25,000
25	Failing to comply with the requirements specified under Article 25 of the Law made for the purpose of this Law	$25,000
26	Failing to comply with the requirements specified under Article 26 of the Law made for the purpose of this Law	$25,000

2. Legal basis for processing of Special Categories of Personal Data

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.
Article 3 of Schedule 1 of the Data Protection Law defines Special Categories of Personal Data as the "Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership 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".
Article 11 of the Data Protection Law sets out the legal bases for processing of Special Categories of Personal Data.

Processing of Special Categories of Personal Data shall not be processed unless for one or more specifies purposes:

2.1 Explicit consent

A Data Subject has given explicit consent that complies with Article 12 of the Law, to the Processing of those Special Categories of Personal Data for one or more specifies purposes.

2.2 Processing is necessary in the context of employment relationship

Processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of a Data Controller or a Data Subject in the context of the Data Subject's employment, including but not limited to recruitment, visa or work permit processing, the performance of an employment contract, termination of employment, the conduct of proceedings relating to employment and the administration of a pension, retirement or employee money purchase benefit scheme (Data Protection Law, Art 11 (b)).

2.3 Processing is necessary to protect the vital interests of a Data Subject

Processing is necessary to protect the vital interests of a Data Subject or another natural person, where the Data Subject is physically or legally incapable of giving consent (Data Protection Law, Art. 11d)).

2.4 Processing relates to public information

Processing relates to Personal Data that has been made public by a Data Subject (Data protection Law, Art. 11 e).

2.5 Processing is necessary for the establishment, exercise or defence of legal claims

Processing is necessary for the establishment, exercise or defence of legal claims (including, without limitation, arbitration and other structured and commonly recognized alternative dispute resolution procedures, such as mediation) or is performed by the Court acting in its judicial capacity (Data Protection Law, Art. 11 (f)).

2.6 Processing is necessary to comply with a specific requirement of Applicable Law

Processing is necessary for compliance with a specific requirement of Applicable Law to which a Data Controller is subject, and in such circumstances the Data Controller must provide a Data Subject with clear notice of such Processing as soon as reasonably practicable unless the obligation in question prohibits such notice being given. (Data protection Law, Art. 11 g).

2.7 Processing is necessary to comply with regulatory requirements or to prevent or detect a crime

According to Art. 11h) Data Protection Law, Special Categories of Personal Data shall not be processed unless the processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financial obligations or the prevention or detection of any crime that apply to a Data Controller.

2.8 Processing is required for medical purposes

Due to the nature of Natixis' business, it is unlikely to have to process Special Categories of Personal Data for medical purposes. Article 11 i) of the Data Protection Law, which provides a legal basis for such processing is cited here for the sake of completeness. Under this Article, the processing of Special Categories of Personal Data is permitted if it is required for the purposes of preventive, medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Special Categories of Personal Data is processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy. (DIFC Data Protection Law, Art. 11 i).

2.9 Processing is required to protect members of the public

Article 11 j) of the DIFC Data Protection Law, sets out a legal basis for processing Special Categories of Personal Data when the processing is required for protecting members of the public against:

(a) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, management consultancy, IT services, accounting or other commercial activities (either in person or indirectly by means of outsourcing);

(b) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, financial or other services.

(DIFC Data Protection Law, Art. 11j).

2.10 Processing is necessary to protect a Data Subject

Processing is proportional and necessary to protect a Data Subject from potential bias or inaccurate decision making, where such risk would be increased regardless of whether Special Categories Personal Data is Processed. (DIFC Data Protection Law, Art. 11k).

2.11 Processing is necessary for substantial public interest reasons

Processing is necessary for substantial public interest reasons that are proportionate to the aim(s) pursued, respect the principles of data protection and provide for suitable and specific measures to safeguard the rights of the Data Subject. (DIFC Data Protection Law, Art. 11l).

3. Data Subjects rights and exemptions

This section supplements section 5.1.1.3 of the main body of the Global Data Privacy Policy.
Part 6 of the Data Protection law provide the Data Subject with:

3.1 Right to withdraw consent (Article 32)

Where the basis for the Processing of Personal Data is consent under Article 10(1)(a) or under Article 11(1)(a), the Data Subject may withdraw consent at any time by notifying the Data Controller in accordance with Article 12(5).

Where a Data Controller has not complied with Article 12(5) a Data Subject may notify the Data Controller by any reasonable means.

The right to withdraw consent is an absolute right available to a Data Subject if the basis for the Processing of the Data Subject's Personal Data is consent under Article 10(1)(a) or Article 11(1)(a).

Upon the exercise of a Data Subject's right to withdraw consent, a Data Controller must comply with Article 22 and must cease Processing the Personal Data as soon as reasonably practicable and ensure that any Processors do the same.

3.2 Rights to access, rectification and erasure of Personal Data (Article 33)

Data subjects have a right to access copies of their personal data by making a written request to the Data Controller. The initial request is free, though a charge can be made for subsequent requests. Data Controllers may refuse the request if it is manifestly unfounded or excessive. The response must be provided within a month, though this can be extended by two months if the request is complex.

A Data Subject has the right to require the Data Controller to erase his personal data in certain circumstances. However, those circumstances are relatively limited, for example, where the processing is no longer necessary in relation to the purposes for which it was collected, the processing is unlawful or, where the processing was based on consent, that consent is withdrawn and there are no other grounds for processing. Even where the right does arise, there are a range of exemptions, for example where there is a legal obligation to retain the personal data or where its erasure is not feasible for technical reasons (provided certain conditions related to disclosure are satisfied).

3.3 Objection to direct marketing (Article 34)

A Data Subject has the right to be informed before personal data is used on their behalf for the purposes of direct marketing. A Data Subject must also be expressly given the right to object to such use. A Data Subject can object to their personal data being processed for direct marketing purposes at any time. This includes profiling to the extent related to direct marketing.

3.4 Rights to data portability (Article 37)

Data subject will also have a right to data portability where the condition for processing personal data is consent or the performance of a contract and is carried out by automated means. It entitles individuals to obtain any personal data they have provided to the Data Controller in a structured, commonly used and machine-readable format. Individuals can also ask for personal data to be transferred directly from one Data Controller to another.
A Data Controller is not required to provide or transmit personal data where doing so would infringe the rights of any other natural person.

3.5 Other rights

The Data Protection Law contains a number of other rights including the right to request the rectification, or restricting the use, of personal data where the processing does not comply with the provisions of the Data Protection Law. There is also a right to object to processing being carried out in the performance of a task carried out in the public interest or under the legitimate interests' condition.

Finally, a Data Subject may not to be discriminated against for exercising his rights under the Data Protection Law (Article 39).

4. Data Controller's obligations

4.1 Data Controller's obligation to notify

The Data Controller shall communicate any rectification or erasure of Personal Data or Processing restriction carried out in accordance with Articles 33, 34 and 35 to each recipient to whom the Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort. A Data Controller shall inform the Data Subject about those recipients if a Data Subject requests it.

4.2 Notice of breach laws

A Data Controller must notify the Commissioner of a personal data breach which compromises a Data Subject's confidentiality, security or privacy, as soon as practicable.

A Data Controller must notify the Data Subject, as soon as practicable, if the breach is likely to result in a high risk to his security or rights and promptly if there is any immediate risk of damage to the Data Subject.

5. Data Transfers

This section supplements section 9 of the main body of the Global Data Privacy Policy.

Before transferring Personal Data to a jurisdiction outside the DIFC, even if it is within the UAE, Natixis must ensure that this jurisdiction has an adequate level of protection for that Personal Data and that it is listed as an acceptable jurisdiction under the DPR or any other jurisdiction as approved by the Commissioner of Data Protection. (Data Protection Law, Art 26). See also Regulations App3 for a list of acceptable jurisdictions).
A transfer of Personal Data to a jurisdiction that does not have an adequate level of protection may still take place provided some conditions are met (Data Protection Law, Art 26). Since Natixis offers life insurance and health insurance, it may also be worth noting the data localization requirement included in *Federal Law No.2/2019 On the Use of the Information and Communication Technology (ICT) in Health Fields*. According to Article 13 of this law, health information and data related to health services provided in the UAE may not be stored, processed, generated or transferred outside of the UAE, unless otherwise stated by virtue of a decision issued by any Federal or local governmental health authority in the UAE or the Ministry of Health and Prevention.