EMPLOYEES' PERSONAL DATA PROTECTION NOTICE

The protection of your personal data is important to the BNP Paribas Group, which has adopted strong principles in that respect for the entire Group in its Group Privacy Policy available at Echonet > Useful Links > Employees' personal data.

This Data Protection Notice provides you with transparent and detailed information relating to the protection of your personal data by BNP Paribas SA and/or its subsidiaries as your employer ("**we**").

This Data Protection Notice applies to all BNP Paribas 'current and former employees, with open-ended contract or fixed term contract, the trainees, the temporary staff, the apprentices, the vacation workers, persons under "VIE" contract (Volontariat International en Entreprise), ("**you**"). External contractors are expressly excluded from the scope of this Data Protection Notice.

We are responsible, as a controller, for collecting and processing your personal data, in relation to our activities.

For France, we may be responsible for joint processing of certain personal data processing.

This Data Protection Notice lets you know which personal data we collect about you, the reasons why we use and share such data, how long we keep it, what your rights are and how you can exercise them.

This Data Protection Notice may be supplemented by other local statements (Local Employee Data Protection Add-on, Terms and Conditions or Notices) as it is required to comply with local law in the country where you live and/or work, or where employees' representation agreements exist.

For further information, please refer to the Group Human Resources (GHR) policy « General Policy of the BNP Paribas Group on HR Personal Data Protection – RHG0055 ».

1. WHICH PERSONAL DATA DO WE COLLECT AND USE ABOUT YOU?

We collect and use the following categories of personal data (meaning any information that identifies or allows identifying you), to the extent necessary for the purposes detailed in section 3.

Depending on the nature of our employment relationship with you, we may collect and use various types of personal data, about you including:

- **identification information** (e.g. full name, identity (e.g. ID card, and passport information), nationality, place and date of birth, gender, photograph, video, UID);
- **private and professional contact details** (e.g. postal and e-mail addresses, phone number, emergency contact details);
- **family situation** (e.g. marital status, dependents and their dates of birth);
- **social insurance number/national insurance number/identification number;**
- **tax information and debt status** (e.g. tax ID, tax status);
- **recruitment information** (e.g. level of education, CV's, professional qualifications, cover letter, interview .)
- **employment information and data related to your career within BNP Paribas** (e.g. appraisals, performance information, disciplinary and grievance measures, violations of the code of conduct and/or company policies and procedures; compensation/remuneration, internal

appointments, office location, information about training, absence record, note feedback, report of the job interviews, skills self declared in BNP Paribas tools);

- **financial data** (e.g. bank account details and other information necessary to administer payroll, taxes, retirement, pension and benefits);
- **information related to your work permit** (e.g. immigration and residence status information);
- **information related to the management of occupational health and to work-related illnesses and occupational incidents;**
- **data related to the work organization** (e.g. professional agenda, time recording, connection logs, accreditations, absence, leaves);
- **data related to the provision of professional equipment and devices** (e.g. IP address, driving license, equipment provided to the employee (e.g. vehicles, laptops, smartphones, business cards));
- **data related to professional representation with regards to your Employer** (e.g. union representatives' election, information relating to the management of working time);
- **business travels** (e.g. travel details and preferences, visa related information, business expenses);
- **recording of data images and sounds** (e.g including video surveillance using CCTV (Closed Circuit TeleVision), video photograph professional photos, phone calls, electronic conversation and communications);
- **geolocation data** (e.g. through your professional phone, your professional laptop, swipe card record and/or roaming status through our corporate device);
- **social networks data** (e.g. LinkedIn profile) when it is public and authorized by Terms and Conditions of the social networks.

We may collect and use the following sensitive data only when required by law or when you have given your consent:

- **biometric data and genetic information** (e.g. fingerprint, voice pattern, face pattern which can be used for identification and security purposes);
- **health data**;
- **trade union membership** (pursuant to point (b) of Article 9(2) of the General Data Protection Regulation);
- **information about criminal convictions and offences data.** (e.g. for investigation or background checks);

Unless it is required through a statutory legal obligation or has been made publicly available by you, we do not collect nor process personal data related to your ethnic origins, political opinions, religious or philosophical beliefs data or data concerning your sexual orientation.

2. WHO IS CONCERNED BY THIS NOTICE AND FROM WHOM DO WE COLLECT PERSONAL DATA?

We collect data directly about you as an employee but also indirectly to other persons related to you. Thus, we collect information about individuals whereas they have no direct relationship with us but are related to you, such as for instance your:

- The family members;
- Your employees' debtor (for instance in case of wage withholding);
- The beneficiaries of extra-legal benefits.

When you are providing us personal data about these third parties like the examples listed above, please remember to inform them that we process their personal data and direct them to the present Data Protection Notice.

We may sometimes also collect additional information from third parties such as:

- others BNP Paribas Group entities;
- Background check providers;
- Former employers;
- Trustees/ managers of pension arrangement; and
- Social media and other public sources.

3. WHY AND ON WHICH BASIS DO WE USE YOUR PERSONAL DATA?

a. To comply with our statutory legal and regulatory obligations

As a financial institution and an employer, we use your personal data to comply with various regulatory obligations:

- To prevent market abuse to monitor and record keeping transactions, phone calls and communication (including voice over IP), electronic communications (such as emails, chats emails, SMS…), to identify those which deviate from the normal routine/patterns such as personal transactions;
- To ensure the transparency of financial transactions in markets by monitoring and recording transactions, phone calls and communication (including voice over IP), electronic communications (such as, emails, chats emails, SMS…) when necessary;
- To verify the element necessary for identify control and conduct identity checks;
- to perform background checks for candidates and employees;
- to manage tax calculation and declaration;
- to comply with occupational health and safety obligations;
- to comply with fit and proper requirements for members of the management bodies and key function holders;
- to comply with whistleblowing and conflict of interests obligations;
- to manage the organization of professional elections and of meetings for employee representative bodies ;
- to manage accreditations for security purposes;
- to provide mandatory training to our employees including mandatory training request management ;
- to prevent, detect and report risks related to Corporate Social Responsibilities and sustainable development;
- to comply with regulation relating to sanctions and embargoes;
- to exchange and report different information or reply to official requests from a duly authorised local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, law enforcement, state agencies or public bodies;
- to maintain security e.g. to ensure network and information security, including protecting BNP Paribas Group against malicious and inadvertent data security breaches
- to manage any health situation, such as epidemic or pandemic, in order to guarantee your health and the continuity of our activities and infrastructure.

b. To perform the contract we have entered with you

We use your personal data to enter into and perform your employment contract, including:

- execution of your mission entrusted by your employer
- recruitment and staffing such as applications for CV management ;
- training and mobility management including the recommendation of personalized training and job offers available within the Group;
- administrative management of the employees, including payroll, compensation, target bonus and extra-legal benefits (including compensation metrics and decisions, bonus calculations and stock plan administration, pension and information relating to retirement planning and other insurance schemes and management of your banking account and banking benefits);
- management of occupational health;
- management of performance and, succession planning;
- management of leaves and absences ;
- management of possible grievance or disciplinary hearings ;
- management of general HR administration

Furthermore, your personal data analysis allows to better answer at your expectations in terms of proactivity and personalization.

c. To fulfil our legitimate interest

We also collect and use your personal data where we have a legitimate reason :

- to manage the working time (e.g. the flexible working hours system, facilities occupation rate);
- to ensure physical security of our buildings, in particular video protection and manage building access and office supplies (e.g. badges, access to the company restaurant and cafeteria facilities and the services of the employee representative committee)
- to manage professional expenses ;
- to provide the IT and Telecom equipment's including mobile phones, laptops, vehicles and software's necessary for the employees activities;
- to manage career, appraisals and development skills,
- to manage and to monitor professional device data usage ;
- to manage internal directory and business diary;
- to manage internal communications within the entity (e.g. chat, emails);
- to manage inquiries and surveys ;
- ensure your safety by conducting internal investigations in the event of an incident ;
- to organise events (such as conferences or business meetings);
- to manage authorised signatures and delegations of authority;
- to organize our employees including training request management ;
- to manage file reporting via, for example, a shared platform in order, in particular, to have reports of risks related to files
- to record meetings by videoconference to enable them to be rebroadcast on demand for awareness raising, training, webinars and project management

- to access information from your social network profile (when it is public and authorized by Terms and Conditions of the social network).

- to manage, prevent and detect fraud ;
- to manage, prevent and detect bribery;
- to manage, prevent and detect money laundering and financing of terrorism;
- to comply with regulation relating to sanctions and embargoes when it is required by the applicable law.
- to manage the compliance and risk management, such as background check reports, and security data;
- to record, listen (again) and play back phone calls from our call centers and banking branches for the purpose of training and improving our customer services or to gather evidences;
- to monitor and keep record keeping of phone calls and communication (including voice over IP), of electronic communications (such as, emails, chats emails, SMS…) in order to comply with the Bank's code of conduct and foreign legal and regulatory obligations to which it is subject ;

- to perform your background checks when it is required by applicable law
- to carry out background checks beyond what is require monitor your use of our information and communication systems, including monitoring Internet use and electronic communications (e.g. connection logs for data loss prevention) :
- to monitor your use of our information and communication systems, including monitoring internet usage and electronic communication (e.g. - log for the data loss prevention),
    - using tools such as the Data Leak Detection Tool (DLP) and the application of security rules (such as blocking, scan and quarantine of electronic communications with attachments) in order :
    - to ensure compliance with our internal policies including the Bank's code of conduct;
    - to maintain and comply with our internal obligations of security and confidentiality e.g. to ensure network and information security, including protecting BNP Paribas Group against malicious or inadvertent data security breaches;

In in case of suspicion and/or breach of our IT security rules, we will be able to take the necessary measures (e.g. access to electronic communications and attachments affected by this suspicion and/or offence) in compliance with the regulations in force and the norms and procedures at BNP Paribas.

- to process reports related to your public publications on the social media as part of your obligations of confidentiality and loyalty ;

- to perform the IT management, including infrastructure management (e.g. shared platforms) and business continuity and IT security;
- to manage our defense of legal claims and litigation;
- to detect, manage, prevent and investigate allegations and proven cases of misconduct, or violation of the law, the company's code of conduct and/or company policies and procedures, subject to compliance with our internal policy and local legal requirements,

notably within the framework of a special mission of the General Inspection and/or the implementation of consolidated monitoring tools for such violations.

- To manage recruitment and mobility assistance through the performance of personality tests, matching of personality, comparison of your test result to standard test result;
- to establish aggregated statistics, tests and models (e.g. implementation of chatbots), in order to improve our processes;
- to conduct data analytics studies to review, better understand and monitor for example employee retention and attrition rates;

We can inform and suggest you, without any personal targeting, some Group products and services through professional devices (for example : emails) with preferred employee's terms. You are then free to subscribe or not these offers.
You have the absolute right to object at any time to the processing of your personal data for direct marketing purposes by contacting directly the service at the origin of this processing.

Moreover, you can object also at any time, on grounds relating to your particular situation, to any processing of your personal data.

In any case, our legitimate interests remain proportionate, and we verify according to a balancing test that your interests and fundamental rights are preserved. Should you wish to obtain more information about such balancing test, please contact us using the contact details provided in section 9 "How to contact us" below.

d. To respect your choice if we requested your consent for a specific processing

For certain personal data processing, we will communicate additional information and invite you to consent to such processing (note that you may be able to withdraw your consent at any time) notably:

- where the above purposes lead to automated decision-making, which produces legal effects or which significantly, concern and affects you. In this case, we will inform you separately about the logic involved, as well as the significance and the envisaged consequences of such processing;
- if we need to carry out further processing for purposes other than those above, we will inform you and, where necessary, obtain your consent.

4. WHO DO WE SHARE YOUR PERSONAL DATA WITH?

a. Sharing of information within the BNP Paribas Group

We may share your personal data with BNP Paribas Group entities to fulfill the purposes set out above where it is necessary, including to respect our legal and regulatory obligations (e.g. as part of our regular reporting activities), and/or legitimate interests (e.g. in the context of a business reorganization or group restructuring or for our maintenance information system and the hosting of our data).

b. Disclosing information outside the BNP Paribas Group

In order to fulfil some of the purposes described in the notice, we may disclose from time to time your personal data with third parties including:

- service providers and subcontractors which perform services on our behalf;
- partners and associations with whom we are partnering, or when you choose to participate in any of their events;
- local or foreign financial, tax, administrative, criminal or judicial authorities, regulators, arbitrators or mediators, law enforcement, state agencies or public bodies, where we are required to disclose data pursuant to:
    - their request;
    - defending or responding to a matter, action or proceeding;
    - complying with regulation or guidance from an authority applying to us ;
- certain regulated professionals such as lawyers, notaries', rating agencies or auditors under specific circumstances (e.g. litigation, audit, etc.) or insolvency administrators in case of private bankruptcy;
- garnishes in case of wage garnishments;
- professional associations and pension schemes;
- workers' council;
- health insurance companies/funds, social security agencies.

5. INTERNATIONAL TRANSFERS OF PERSONAL DATA

In case of international transfers originating from the European Economic Area (EEA) to a non-EEA country recognized by the European Commission as providing an adequate level of data protection, your personal data will be transferred on this basis.

For transfers to non-EEA countries where the level of personal data protection has not been recognized as adequate by the European Commission we will either rely on a derogation applicable to the specific situation or implement one of the following safeguards to ensure the protection of your personal data:

- notably by Binding Corporate Rules (BCR) and any supplementary measure as appropriate;
- standard contractual clauses (SCC) and any supplementary measure as appropriate;

To obtain a copy of these safeguards or additional details on where they are available, you can access to the Echonet page (> useful link> Group > employee' personal data.

6. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We will retain your personal data over the period required to comply with applicable laws and regulations or another period to achieve the purpose for which it was collected. For example, the main retention period applied within HR systems is five years after the termination of your employment contract to the extent no diverging local retention periods exist.

7. WHAT ARE YOUR RIGHTS AND HOW CAN YOU EXERCISE THEM?

In accordance with applicable regulations and where applicable, you have the following rights:

- to **access**: you can obtain information relating to the processing of your personal data, and a copy of such personal data;

- to **rectify**: where you consider that your personal data are inaccurate or incomplete, you can request such personal data to be modified accordingly;
- to **erase**: you can require the deletion of your personal data, to the extent permitted by law;
- to **restrict**: you can request the restriction of the processing of your personal data;
- to **object**: you can object at any time, on grounds relating to your particular situation, to the processing of your personal data. In such case, we will no longer process your personal data unless we demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms, or for the establishment, exercise or defense of legal claims. You also have the absolute right to object to the processing of your personal data for direct marketing purposes, which includes profiling related to such direct marketing;
- to **withdraw your consent**: where you have given your consent for the processing of your personal data, you have the right to withdraw your consent at any time;
- to **data portability**: where legally applicable, you have the right to have the personal data you have provided to us be returned to you or, where technically feasible, transferred to a third party.
- to **organize data after death when it is required by law**

If you wish to exercise the rights listed above, please send a letter or e-mail to your contact as referred in the contact list available at Employees' personal data > Contact List. Please include a scan/copy of your proof of identity for identification purpose, when required.

In accordance with applicable regulation, in addition to your rights above, you are also entitled to lodge a complaint with the competent supervisory authority.

8. HOW CAN YOU KEEP UP WITH CHANGES TO THIS DATA PROTECTION NOTICE?

In a world of constant regulatory and technological changes, we may need to regularly update this Notice.

We invite you to review the latest version of this Notice online and we will inform you of any material changes through our website via our other usual communication channels.

9. HOW TO CONTACT US?

If you have any questions relating to our use of your personal data under this Notice contact your Data Protection Officer via the following email address “PARIS RHG RGPD ARTICLES 15 ET 16” who will handle your query.

If you wish to learn more about cookies, please read our cookies policy.