NOTICE ON THE PROTECTION OF PERSONAL DATA FOR THE STAFF OF BNP PARIBAS GROUP'S EXTERNAL SUPPLIERS AND EXTERNAL PARTNERS

The protection of your personal data ("**personal data**") is important to the BNP Paribas Group.

This Data Protection Notice provides you with transparent and detailed information relating to the protection of your personal data by the entities of the BNP Paribas Group ("**we**" or "**us**").

This Data Protection Notice applies to both **permanent and non-permanent staff, ultimate beneficial owners, corporate officers and directors, representatives, agents and/or managers of**:

- **external suppliers** who provide products and/or services to us; or
- **external partners** with which we have a partnership and/or or sponsorship contract.

Hereafter "**you**".

The purpose of this Data Protection Notice is to inform you about the personal data we collect about you, from you and/or from the supplier or partner you represent or work for, the reasons why we use and share such data, how long we keep it, what your rights are and how you can exercise them.

We are responsible, as a controller, for collecting and processing your personal data as set out in the Data Protection Notice.

This Data Protection Notice could be supplemented or specified, if necessary, by other local policies and procedures (such as appendices on the protection of personal data, Terms and Conditions, notices/board in the premises of the entities of BNP Paribas Group, etc.), in particular, as required by local legal and regulatory requirements in the country where the contract is performed.

Should you provide us with third party individual personal data, you must provide a copy of this Data Protection Notice to this individual.

1. WHICH PERSONAL DATA DO WE USE ABOUT YOU?

We collect and use your personal data, meaning any information that identifies or allows us to identify you, the extent necessary in the framework of our activities and to perform services, partnership or sponsorship agreement.

Depending on the nature of the products or services provided by the supplier or partner, we collect various types of personal data about you, including:

- **Identification information** (e.g. full name, ID card, passport information, nationality, place and date of birth, gender, professional photograph);
- **Professional contact information** (e.g. postal and e-mail address, phone number, emergency contact details);
- **Connection and tracking data and information about your device** (e.g. IP address, technical logs, computer traces, information on the use and the security of the device);
- **Education and employment information** (e.g. CV, level of education, professional qualifications and references, date of hire and position held with your employer, information on business travel, details of training or of information session completed where necessary for the performance of

the relevant contract (e.g. in areas such as GDPR, data security, banking and financial sectors when the mission requires it));

- **Your presence in our premises** (e.g. license plate);
- **Data relating to your work permit** (in particular, the type and serial number of a work permit for non-EU citizens when working in the E.U, and residence and immigration status);
- **Data from your interactions with us** (e.g. minutes of meetings, phone calls, videoconferences, electronic communications (emails, instant messaging (chat)…);
- **Images recording** (e. g. video surveillance (CCTV), photos);
- **Social network data** (e.g. data coming from pages and publications on social networks that contain information that you publicly made available).

We may collect the following special categories of data (or "sensitive data") only upon obtaining your explicit prior consent and/or when required by law:

- **Biometric data** (e.g. fingerprint, voice pattern, face pattern or facial recognition which can be used for identification and security purposes); and
- **Data relating to criminal convictions and offences** (e.g. extract of criminal record).

We never ask for any other sensitive personal data such as data related to your racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data or data concerning your sex life or sexual orientation, unless it is required through a legal obligation or if you requested it.

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

We collect data either directly from you or indirectly from the supplier or partner you represent or work for within the framework of a service, partnership or sponsorship agreement that we entered into.

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

In this section, we describe how and why we use your personal data.

a. To comply with our various legal and regulatory obligations

- Manage, prevent and detect fraud;
- Manage, prevent and detect money laundering and financing of terrorism and comply with regulations relating to international sanctions and embargoes through our Know Your Supplier (KYS) procedure;
- Prevent market abuses to monitor and record transactions, phone calls (including VoIP and videoconferences), electronic communications (such as emails, instant messaging (chat), SMS…) in order to identify those which deviate from normal activities and habits such as personal account dealing;
- Ensure transparency of transactions on the financial markets by monitoring and recording transactions, phone calls (including VoIP and videoconferences), electronic communications (such as emails, instant messaging (chat), SMS…) when required;
- Manage, prevent and detect corruption;
- Comply with banking secrecy regulations and prevent any related incident;
- Implement a system for handling professional alerts;
- Exchange information and report on different operations, transactions or requests, or respond to official requests from duly authorized local or foreign judicial, criminal, administrative, tax or

financial authorities, arbitrators or mediators, law enforcement authorities, government bodies or agencies;

- Manage any sanitary situation, such as epidemics or pandemics, in order to ensure your health and our staff's health, as well as the continuity of our information technology tools;
- Prevent, detect and report risks related to our Corporate Social Responsibilities and Sustainable Development;
- Fight against undeclared/illegal work.

b. To perform a contract with you or to take steps at your request before entering into a contract

- Manage our information systems, including infrastructure management, access to specific information technology resources and supplies, and access to workstations or applications (including BNP Paribas related security features) when required for the performance of the services, partnership or sponsorship contract(s);
- Ensure business continuity (e.g. implementation of the Business Continuity Plan) and crisis management;
- Use of purchasing management tool to enable monitoring of the entire procurement cycle from purchase requisition to the invoice (including in particular the provision of supplier catalogues and contracts, the management of invitations to tender and the receipt of purchase orders);
- Follow-up on the provision of products or services, including checkpoint meetings to review the progress made;
- Panel our suppliers and partners;.
- Manage accounting, billing, payment of fees and taxes, and monitor the payments in order to comply with our internal and legal procedures.

c. To fulfil our legitimate interest

- Ensure physical security of our buildings, including in particular video protection and management of supplier or partner's staff authorization for access to certain BNP Paribas buildings and car parks (access badges, security, etc.);
- Implement an ethical alert treatment management system;
- Manage our information systems, including infrastructure management, access to specific information technology resources and supplies, and access to workstations or applications (including BNP Paribas related security features) when required for the performance of the services, partnership or sponsorship contract(s) we have in place with your employer or the company you represent;
- Ensure business continuity (e.g. implementation of the Business Continuity Plan) and crisis management;
- Use of purchasing management tool to enable monitoring of the entire procurement cycle from purchase requisition to the invoice (including in particular the provision of supplier catalogues and contracts, the management of invitations to tender and the receipt of purchase orders);
- Follow-up on the provision of products or services, including checkpoint meetings to review the progress made;
- Panel our suppliers and partners;.
- Manage accounting, billing, payment of fees and taxes, and monitor the payments in order to comply with our internal and legal procedures.
- Monitor compliance with our internal policies and procedures including but not limited to our code of conduct. This may include monitoring and recording of phone calls and voice

communications (including VoIP and videoconferences), emails and instant messaging (chat) communications when you interact with our employees subject to specific legal and regulatory obligations;

- Record meetings by videoconference to enable them to be rebroadcast on demand for awareness raising, training, webinars and project management;
- Ensure IT security and the provision of IT devices to you for:
    - Monitoring and maintenance of IT tools and professional electronic messaging;
    - Implementation of devices in order to ensure the security and proper functioning of IT applications and networks;
    - Definition of access authorizations to the applications and to the networks;
- Monitor your use of our information and communication systems, including monitoring internet usage and electronic communication (e.g. - log for the prevention of data loss), 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 incorporating attachments) to:
    - Ensuring compliance with our internal policies, including the Bank's Code of Conduct;
    - Maintain and respect our internal security and confidentiality obligations, e.g. ensuring network and information security, including protection of the BNP Paribas Group against malicious and unintentional data security violations
- Take the necessary measures in the event of suspicion and/or breach of IT security rules (e.g. access to electronic communications and attachments concerned per such suspicion and/or infringement) in accordance with applicable regulations and BNP Paribas standards and procedures;
- Manage our procedures, in particular in terms of health and safety at work and IT security rules;
- Manage awareness on cybersecurity and personal data protection principles;
- Comply with the regulations on sanctions and embargoes beyond what is required by applicable law;
- Ensure communication of information to administrative authorities (e.g. for insider trading);
- Ensure our defense in the event of legal claims and against litigation and lawsuits;
- Manage our activities and our presence on social networks.

In any case, our legitimate interest remains proportionate and we verify, according to a balancing test, that your interests or fundamental rights and freedoms 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 request your consent for a specific processing

For certain types of personal data processing for purposes other than those provided for in Section 3, we will provide you with specific information and invite you to consent to such processing. Please note that you may revoke your consent at any time.

4. WHO DO WE SHARE YOUR PERSONAL DATA WITH?

a. Sharing of information within the BNP Paribas Group

In the course of our activities, and in order to fulfill the purposes listed in this Data Protection Notice, we may share your personal data within the BNP Paribas Group entities.

b. Disclosing information outside the BNP Paribas Group

In order to fulfill some of the purposes described in this Data Protection Notice, from time to time we may disclose your personal data to:

- our suppliers and subcontractors who provide services and products on our behalf (e.g. IT systems providers, cloud service providers, database providers, security and facility management providers);
- Companies you represent or work for;
- local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, law enforcement, state agencies, fraud prevention agencies or public bodies, we or any member of the BNP Paribas Group are required to disclose to pursuant to:
    - their request;
    - defend or respond to a matter, action or proceeding; and/or
    - comply with regulation or guidance from authorities applying to us or any member of the BNP Paribas Group;
- any third party to whom we assign or novate any of our rights or obligations;
- certain regulated professionals such as lawyers, notaries, rating agencies or auditors, when specific circumstances require it (litigation, audits, etc.) as well as to any current or potential buyer of the companies or activities of the BNP Paribas Group or our insurers.

5. INTERNATIONAL TRANSFERS OF PERSONAL DATA

In certain circumstances (e.g. to provide international services or to ensure operational efficiency), we may transfer your data to another country.

In case of international transfers originating from:

- the European Economic Area ("EEA") to a non-EEA country, the transfer of your personal data may take place where the European Commission has recognised a non-EEA country as providing an adequate level of data protection. In such cases your personal data may be transferred on this basis;
- the United Kingdom ("UK") to a third country, the transfer of your personal data may take place where the UK Government has recognised the third country, as providing an adequate level of data protection. In such cases your personal data may be transferred on this basis;
- other countries where international transfer restrictions exist, we will implement appropriate safeguards to ensure the protection of your personal data.

For other transfers, we will implement an appropriate safeguard to ensure the protection of your personal data, being:

- Standard contractual clauses approved by the European Commission or the UK Government (as applicable); or
- Binding corporate rules.

In the absence of an adequacy decision or an appropriate safeguard we may rely on a derogation applicable to the specific situation (e.g., if the transfer is necessary for the exercise or defense of legal claims).

To obtain a copy of these safeguards measures to ensure the protection of your personal data, or to obtain details on where they are available, you can send a written request as set out in Section 9.

6. HOW LONG DO WE KEEP YOUR PERSONAL DATA FOR?

We keep personal data for as long as we have a contractual relationship with the supplier/ partner you represent or work for. After our contractual relationship ends, we will retain your personal data, (I) during the period required to comply with applicable laws and regulations; or (ii) for a defined time period, such as to assert legal claims or to respond to requests from regulatory bodies.

For example:

- Your data is kept for the duration of your mission and is deleted at the latest 3 years after the end of the mission performed for us on behalf of your employer except if the law requires a longer period,
- Video protection data is kept during a month, then deleted, unless required, in particular, for the establishment, exercise or defense of legal claims.

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

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

- to **access**: you may have the right to 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 that such personal data be modified accordingly;
- to **erase**: in some circumstances, you can require the deletion of your personal data, to the extent permitted by law;
- to **restrict**: in some circumstances, you can request the restriction of the processing of your personal data;
- to **object**: in some circumstances, you can object to the processing of your personal data, on grounds relating to your particular situation;
- to **give instructions**: related to the conservation, the erasure or the communication of your data, after your death;
- 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 can ask the restitution of personal data you have provided to us, where technically feasible, the transfer of personal data to a third party.

If you wish to exercise these rights, please refer to section 9 hereafter. For identifications purposes, we may ask you for a proof of your identity.

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 technological change, we may need to update this Data Protection Notice from time to time.

We invite you to review the latest version of this notice online and we will inform you of any material changes through our website or through 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 Data Protection Notice or if you wish to exercise the rights described in section 7, please contact the data protection office of the BNP Paribas entity you are working with/for.

You can ask your usual point of contact at BNP Paribas for the contact details of the data protection office. If you don't have a point of contact at BNP Paribas, please reach out to your employer for support.

As a last resort, if you can't retrieve the data protection office's contact details of the BNP Paribas entity you are working with/for, please send an email to group.supplierspersonaldata@bnpparibas.com with the name and location of the BNP Paribas entity you are working for/with.

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