Data Protection Notice

Employees of service providers, partners and agents of la Financière des Paiements Électroniques

This English version is provided for convenience purposes and only has an informative value.

Please note that only the French version has a contractual value and is binding towards us.

Last update date: 13th July 2023

La Financière des Paiements Électroniques ("**Nickel**") attaches great importance to the protection of your personal data ("**personal data**").

This Data Protection Notice provides clear and detailed information about how personal data is protected by Nickel ("**we**").

This Data Protection Notice applies to **permanent and non-permanent employees, beneficial owners, corporate officers as well as representatives, managers and/or executive officers of**:

- **service providers** with whom we intend to enter into or have entered into a contract for the provision of services and/or the supply of goods on our behalf;
- **partners** with whom we intend to conclude or have concluded a partnership agreement;
- **agents** providing payment services (also called distributors) with whom we intend to conclude or have concluded an agent agreement ("**you**").

As such, this Notice informs you about the personal data we collect about you, from you and your employer, if any, the purposes for which we use and share it, how long we keep it, what your rights are and how you can exercise them.

As data controller, we are responsible for the collection and processing of your personal data as described in this notice.

This notice may be clarified or supplemented, if necessary, by other provisions at local level (specific appendices on the protection of personal data, general conditions of use) in particular in order to comply with the legal obligations of the country where you carry out your mission.

Nickel brings the notice to the attention of the service provider, partner, or agent, who will have to provide you with it before any execution of your mission.

1. WHAT TYPES OF YOUR PERSONAL DATA DO WE USE?

We collect and use your personal data, i.e. any information that identifies you or enables you to be identified that is necessary to provide services, supply goods, perform the partnerships or distribute Nickel products and services.

Depending in particular on your mission, we collect different types of personal data about you, including:

- **Identification information** (e.g. name, surname, ID card and passport number, nationality, date and place of birth, sex, professional photograph);
- **Business contact information** (e.g. postal and email address, landline and/or mobile phone number, emergency contact person(s));
- **Identification data** (e.g. IP address, technical logs, computer tracks, information on security and use of the connection terminal);
- **Information relating to training and employment** (e.g. date of hire and position held with your employer, data on business travel, completion of training required to carry out the missions (e.g. GDPR training, data security training, training in banking and finance when required by the mission, etc.);
- **Information on professional background and experience** (resume);
- **Time spent on the premises of Nickel**;
- **Data on your administrative situation** (including type and serial number of the title equivalent to a work permit for non-European Union nationals, residence and immigration status);
- **Data collected in the context of our exchanges with you** (e.g. meeting minutes, telephone conversations, instant messaging);
- **Recording of images** (e.g. video-surveillance, photographs, videos);
- **Social network data** (e.g. data from social network pages and publications containing information that you have made public).

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

- **Data relating to convictions and criminal offenses** (e.g. an extract from the criminal record).

We never ask you to provide us with other sensitive data such as data concerning your racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data or data concerning your life or sexual orientation, unless we are obliged to do so by law or you have requested it.

2. FROM WHOM DO WE COLLECT PERSONAL DATA?

We collect data directly from you and indirectly from your employer in the context of services, partnership or agent agreement concluded with the latter.

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

In this section, we explain how and for what purposes we use your personal data. For example, we use your personal data to:

- comply with our various legal or regulatory obligations
    - manage, prevent and detect fraud;

- manage, prevent and detect money laundering and the financing of terrorism and comply with all regulations relating to international sanctions and embargoes as part of our Know Your Supplier (KYS) and Know Your Intermediaries (KYI) procedure;
- manage, prevent and detect corruption;
- manage, prevent and detect breaches in the field of employment law;
- comply with professional secrecy regulations and prevent any incidents;
- exchange and report different operations, transactions or requests or respond to an official request from a duly authorized local or foreign judicial, criminal, administrative, tax or financial authority, an arbitrator or mediator, law enforcement authorities, government bodies or public agencies;
- manage any health situation, such as epidemics or pandemics, in order to ensure your health and that of our staff and the proper continuity of our IT tools;
- manage, prevent and detect all risks related to Corporate Social Responsibility and sustainable development.

- allow the performance of pre-contractual measures or of the services, partnership or agent agreement
  - management of our information systems including infrastructure management, access to certain IT resources and supplies as well as to workstations or applications when the performance of the contract(s) so require;
  - use of a procurement management tool for Nickel to monitor the entire order cycle from procurement request to invoice payment (including the provision of supplier catalogs and contracts, the management of calls for tender and the receipt of purchase orders);
  - mission follow-up, in particular meetings to review the progress of the mission;
  - selection of providers (including during the tendering process), referencing of partners or agents; or negotiation by mutual agreement in progress or to come;
  - accounting, invoicing, payment of fees and taxes and the monitoring of these payments in order to comply with our internal procedures and/or legal procedures;
  - completing your onboarding process to become a Nickel payment services agent by:
    - ensuring the processing of your requests;
    - verifying the validity of the information required for the constitution of your registration file with the Autorité de Contrôle Prudentiel et de Résolution (ACPR);
    - creating and managing your agent account and your access to your online space on our website.

- the pursuit of our legitimate interest
- physical security of our buildings, including in particular video protection and the management of your authorisations for the access to certain Nickel buildings and floors (access badges, security etc.);
- implement a system for managing the processing of ethical alerts;
- ensure business continuity (implementation of the Business Continuity Plan) and crisis management;
- monitoring compliance with our internal policies and procedures, in particular our code of conduct;
- recording meetings by videoconference to enable them to be replayed on demand for the purposes of awareness-raising, training, setting up webinars and project management;
- IT security and the provision of IT tools to you:
  - Monitoring and maintenance of IT tools and professional electronic messaging system;
  - Implementation of measures to ensure the security and proper functioning of IT applications and networks;

- Definition of access authorisations to applications and networks;

- monitor your use of our information and communication systems, including monitoring internet usage and electronic communication (e.g. connection logs to prevent data loss), using tools such as the data leak detection tool and applying security rules (such as blocking, scanning and quarantining electronic communications containing attachments) in order to:
  - ensure compliance with our internal policies, including the BNP Paribas Group Code of Conduct;
  - maintain and comply with our internal security and confidentiality obligations, such as ensuring network and information security, including protecting the BNP Paribas Group from malicious or inadvertent data security breaches;
- In the event of a suspicion and/or breach of IT security rules, we may take the necessary measures (e.g. access to electronic communications and attachments affected by the suspicion and/or breach) in accordance with applicable regulations and BNP Paribas standards and procedures;
- manage our health and safety at work and the IT security rules in force;
- manage awareness of principles relating to cybersecurity and the protection of personal data;
- comply with regulations relating to sanctions and embargoes beyond what is required by applicable law;
- ensure the communication of information to the competent administrative authorities;
- defend ourselves in the event of legal claims, disputes and legal proceedings;
- manage our presence and activities on social networks.

In all cases, our legitimate interest remains proportionate and we ensure, through a balancing test, that your interests or fundamental rights are preserved. If you would like further information about the balancing test, please contact us using the contact details in section 9 "How to contact us" below.

- Respect your choice when we have asked for your consent for a specific treatment

In the context of certain activities involving the processing of personal data, we may send you specific information and invite you to consent to this processing.

Please note that you can withdraw this consent at any time.

4. WITH WHOM DO WE SHARE YOUR PERSONAL DATA?

a. Data sharing within the BNP Paribas Group

As part of our activities and in order to fulfill the above-mentioned purposes, we may share your personal data with entities of the BNP Paribas Group.

b. Sharing of data outside the BNP Paribas Group

In order to fulfill some of the purposes set out in this notice, we may, from time to time, share your personal data with:

- service providers and subcontractors who perform provide products and services on our behalf (e.g. IT service providers, cloud service providers);
- partners, where you have given your consent for your data to be passed on to them for marketing purposes;
- companies that you work for or represent;

- financial, tax, administrative, criminal or judicial, or local or foreign authorities, arbitrators or mediators, law enforcement authorities, governmental agencies or public bodies, to whom we or, where applicable, any member of the BNP Paribas Group, are required to disclose data:
    - at their request ;
    - in the course of defending or responding to a question, action or proceeding.
    - in order to comply with a regulation or recommendation issued by a competent authority towards us or in respect of any member of the BNP Paribas Group, if applicable;
- any third party to whom we assign or novate our rights and obligations;
- certain regulated professionals such as lawyers, notaries or statutory auditors when required by specific circumstances (litigation, audit, etc.) as well as any current or potential purchaser of Nickel or its activities or our insurers.

5. TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

In case of international transfers from the European Economic Area (EEA) to a non-EEA country, the transfer of your personal data may take place on the basis of a decision of the European Commission, where the European Commission has recognised that the country to which your data will be transferred provides an adequate level of protection.

In the event of a transfer of your data to a country where the level of protection of your data has not been recognised as adequate by the European Commission, we will either rely on a derogation applicable to the specific situation (e.g. if the transfer is necessary to perform a contract concluded with your employer) or we will take one of the following measures to ensure the protection of your personal data:

- standard contractual clauses approved by the European Commission or any additional measures if necessary;
- binding corporate rules.

To obtain a copy of these measures to ensure the protection of your data or to receive details of where your data can be accessed, you may send us a written request as set out in Section 9 below.

6. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We retain your personal data for the period corresponding to the contractual relationship we have with the provider/partner/agent for whom you work or whom you represent. At the end of the contractual relationship, we retain your personal data (i) as long as is necessary to comply with applicable laws and regulations, or (ii) for a defined period of time, in particular to enforce legal rights or respond to requests from regulatory bodies.

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

In accordance with the legislation applicable to your situation, you may exercise, as the case may be, the following rights:

- Right of **access**: you can obtain information concerning the processing of your personal data and a copy of them;

- Right of **rectification**: if you consider that your personal data is inaccurate or incomplete, you may request that it be amended accordingly;
- Right of **deletion**: you may request the deletion of your personal data, within the limits permitted by law;
- Right to **limitation of processing**: you may request limitation of the processing of your personal data;
- Right to **object**: you may object to the processing of your personal data for reasons relating to your particular situation;
- Right to **define guidelines** for the storage, deletion or communication of your personal data, applicable after your death;
- Right to **withdraw your consent**: if you have given your consent to the processing of your personal data, you may withdraw this consent at any time;
- Right to the **portability of your data**: where permitted by law, you may request the return of the personal data you have provided us with or, where technically possible, the transfer of such data to a third party.

If you wish to exercise these rights, please refer to section 9 below. To identify you, we may ask you for a scan/copy of your proof of identity.

In accordance with applicable legislation, in addition to the rights mentioned above, you may lodge a complaint with a competent supervisory authority.

8. HOW CAN I BE INFORMED OF CHANGES TO THIS PRIVACY NOTICE?

In a world where technology is constantly evolving, we may need to update this notice on a regular basis.

We invite you to read the latest version of this document online, and we will inform you of any significant changes through our website or through our usual communication channels.

9. HOW TO CONTACT US

If you have any questions about our use of your personal data under this Data Protection Notice or if you wish to exercise the rights described in section 7, you can contact our Data Protection Officer at donneespersonnelles@nickel.eu , who will deal with your request.

If you would like to know more about cookies, please consult our usage policy https://nickel.eu/fr/politique-dutilisation-des-cookies.