

Information Notice regarding the protection of personal data *Clients and prospects*

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.

The protection of your personal data is at the heart of our concerns. The Financière des Paiements Électroniques (Nickel), a simplified joint stock company, whose registered office is at 1 place des Marseillais, 94220 CHARENTON-LE-PONT (“Us”), is responsible for the processing of your personal data within the framework of its activities.

We are part of the BNP Paribas Group. The purpose of this notice is to explain how we process your personal data and how you can control and manage it.

This notice applies uniformly to all Nickel products and services, although additional information may be provided to you if necessary when you sign up for a particular product or service.

This notice provides answers to the following questions:

Table of contents

1. Are you subject to this notice?	2
2. How can you control the processing activities we do on your personal data?	2
2.1. Right of Access	2
2.2. Right to correct	2
2.3. Deletion right	2
2.4. Right to object to the processing of your personal data based on legitimate interests	3
2.5. Right to object to the processing of your personal data for commercial prospecting purposes	3
2.6. Right to suspend the use of your personal data	3
2.7. Rights against an automated decision	3
2.8. Right to withdraw your consent	3
2.9. Right to request the portability of your personal data	3
3. Why and on which legal basis do we use your personal data?	3
3.1. To comply with our various legal and regulatory obligations	3
3.2. For anti-money laundering and countering of the financing of terrorism purposes	4
3.3. To perform a contract to which you are a party or pre-contractual measures taken at your request	4
3.4. To fulfil our legitimate interest or that of a third party	4
3.5. Respect your choice when you have consented to a specific treatment	5

4. What type of data do we collect?	5
Direct collection	5
Indirect collection	6
5. From whom do we collect personal data from?	6
6. With whom do we share your personal data?	6
7. International transfers of personal data	7
8. How long do we store your personal data?	7
9. How to follow the evolution of this privacy notice?	7
10. How to contact us?	7
Schedule 1 - Processing of personal data to combat money laundering and the financing of terrorism	8
Schedule 2 - Data retention periods	10

1. Are you subject to this notice?

This Privacy Notice applies to you if you are ("**You**"):

- one of our customers;
- a member of our customer family. Indeed, our customers may occasionally share with us information about their family when it is necessary to provide them with a product or service or to get to know them better;
- a person interested in our products or services when you provide us with your personal data (in an agency, on our websites and applications, during events or sponsorship operations) so that we can contact you.

When you provide us with personal data related to other people, please make sure that you inform them about the disclosure of their personal data and invite them to read this Privacy Notice. We will ensure that we will do the same whenever possible (e.g., when we have the person's contact details).

2. How can you control the processing activities we do on your personal data?

You have rights that allow you to exercise meaningful control over your personal data and how we process it.

If you wish to exercise the rights described below, please send us an email request to donneespersonnelles@nickel.eu with a copy of your identification attached. This document confirms that you are the originator of the request and allows us to process it as soon as possible.

If you have any questions regarding the use of your personal data under this notice, please contact our Data Protection Officer at the following address: donneespersonnelles@nickel.eu.

In addition to the rights mentioned below, you may lodge a complaint with the CNIL (Commission Nationale de l'Informatique et de Libertés).

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

2.1. Right of Access

You can directly access some data from your client account on our website or via the Nickel mobile application.

If you wish to have access to your personal data, we will provide you with a copy of the personal data you requested as well as information relating to their processing, on your explicit request.

Your right of access may be limited in the cases foreseen by laws and regulations. This is the case with the regulation relating to anti-money laundering and countering the financing of terrorism, which prohibits us from giving you direct access to your personal data processed for this purpose. In this case, you must exercise your right of access with the CNIL, which will request the data from us.

2.2. Right to correct

Where you consider that your personal data are inaccurate or incomplete, you can request that such personal data be modified or completed accordingly. In some cases, supporting documentation may be required.

2.3. Deletion right

If you wish, you may request the deletion of your personal data, to the extent permitted by law.

2.4. Right to object to the processing of your personal data based on legitimate interests

If you do not agree with a processing activity based on a legitimate interest, you can object to it, on grounds relating to your particular situation, by informing us precisely of the processing activity involved and the reasons for the objection. We will cease processing your personal data unless there are compelling legitimate grounds for doing so or it is necessary for the establishment, exercise or defense of legal claims.

2.5. Right to object to the processing of your personal data for commercial prospecting purposes

You have the right to object at any time to the processing of your personal data for commercial prospecting purposes, including profiling, insofar as it is linked to such prospecting.

2.6. Right to suspend the use of your personal data

If you question the accuracy of the personal data we use or object to the processing of your personal data, we will verify or review your request. You may request that we suspend the use of your personal data while we review your request.

2.7. Rights against an automated decision

As a matter of principle, you have the right not to be subject to a decision based solely on automated processing based on profiling or otherwise that has a legal effect or significantly affects you. However, we may automate such a decision if it is necessary for the entering into or performance of a contract with us, authorised by regulation or if you have given your consent.

In any event, you have the right to challenge the decision, express your views and request the intervention of a competent person to review the decision.

2.8. Right to withdraw your consent

If you have given your consent to the processing of your personal data, you can withdraw this consent at any time.

2.9. Right to request the portability of your personal data

You may request a copy of the personal data you have provided to us in a structured, commonly used and machine-readable format. Where technically feasible, you may request that we provide this copy to a third party.

3. Why and on which legal basis do we use your personal data?

In this section we explain why we process your personal data and the legal basis for doing so. Your personal data is processed :

3.1. To comply with our various legal and regulatory obligations

Your personal data are processed where necessary to enable us to comply with the regulations to which we are subject, including banking and financial regulations.

We use your personal data to:

- monitor operations and transactions to identify those which deviate from the normal routine/patterns (e.g., when you withdraw a large sum of money in a country other than your place of residence);
- manage and report risks (financial, credit, legal, compliance or reputational risks etc.) that the BNP Paribas Group could incur in the context of its activities;
- detect and prevent corruption;
- assist the fight against tax fraud and fulfill tax control and notification obligations;
- record transactions for accounting purposes;
- prevent, detect and report risks related to Corporate Social Responsibility and sustainable development;
- detect and prevent bribery;
- comply with the provisions applicable to trust service providers issuing electronic signature certificates;
- exchange and report different operations, transactions or orders or reply to an official request from a duly authorized local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, law enforcement, state agencies or public bodies.

3.2. For anti-money laundering and countering of the financing of terrorism purposes

As part of a banking Group, we must have a robust system of anti-money laundering and countering of terrorism financing (AML/TF) in each of our entities managed centrally, as well as a system for applying local, European and international sanctions.

In this context, we are joint controllers with BNP Paribas SA, the parent company of the BNP Paribas Group (the term "We" in this section also includes BNP Paribas SA).

The processing activities performed to meet these legal obligations are detailed in **Schedule 1**.

3.3. To perform a contract to which you are a party or pre-contractual measures taken at your request

Your personal data are processed when they are necessary for the conclusion or execution of a contract to:

- subscribe (in particular by electronic signature) to products and services distributed by Nickel;
- provide Nickel's products and services in accordance with the General Terms and Conditions and Tariffs, in particular to enable you to pay and be paid;
- respond to your requests and assist you in your dealings;
- ensure the settlement of your estate.

3.4. To fulfill our legitimate interest or that of a third party

Where we base a processing on legitimate interest, we will balance that interest against your interests or fundamental rights and freedoms to ensure that there is a fair balance between them. If you would like more information about the legitimate interest pursued by a processing, please contact us using the contact details provided in Section 10 "How to contact us" below.

3.4.1 In the framework of our business as a payment service provider we use your personal data to:

- Manage the risks to which we are exposed:
 - o we keep evidence of transactions, including in electronic format;
 - o monitor your transactions to manage, prevent and detect fraud;
 - o we collect debts;
 - o process legal claims and defences in the event of litigation;
- Improve cybersecurity, manage our platforms and websites, and ensure business continuity;
- Improve the automation and efficiency of our business processes and customer services (e.g., tracking your requests and improving your satisfaction based on data collected during our interactions with you such as emails or chats);
- Assist you in managing your budget by automatically categorizing your transaction data.
- To conduct statistical studies and develop predictive and descriptive models for:
 - o commercial: to identify the products and services we could offer you to best meet your needs, to create new offers or identify new trends among our customers, to develop our commercial policy taking into account our customers' preferences;
 - o security: to prevent potential incidents and improve security management;
 - o compliance (such as anti-money laundering and anti-terrorist financing) and risk management;
 - o combatting fraud;

- Organize contests, promotional operations, conduct opinion and customer satisfaction surveys.

3.4.2 We use your data to perform standard profiling to personalise our products and offers

To enhance your experience and satisfaction, we need to determine which customer group you belong to. For this purpose, we build a standard profile from relevant data that we select from the following information:

- what you have directly communicated to us during our interactions with you or when you subscribe to a product or service;
- resulting from your use of our products or services such as those related to your accounts including the balance of the accounts, regular or atypical movements, the use of your card abroad as well as the automatic categorization of your transaction data (e.g., the distribution of your expenses and your receipts by category as is visible in your customer area);
- from your use of our various channels: websites and applications (e.g., if you are digitally savvy);

Unless you object, we will perform this customization based on standard profiling. We may go further to better meet your needs, if you consent, by performing a tailor-made customization as described below.

3.5. Respect your choice when you have consented to a specific treatment

For certain processing of personal data, we will give you specific information and ask for your consent. We remind you that you can withdraw your consent at any time.

In particular, we ask for your consent for:

- Customized personalization of our offers and products or services based on more sophisticated profiling to anticipate your needs and behavior;
- Any electronic offer of products and services not similar to those you have subscribed to or products and services of our trusted partners;
- Use your navigation data (cookies) for commercial purposes or to enrich the knowledge of your profile.

You may be asked to provide further consent to the processing of your personal data where necessary.

4. What type of data do we collect?

Direct collection

We collect and use your personal data, meaning any information that identifies or allows one to identify you.

Depending among others on the types of product or service we provide to you and the interactions we have with you, we collect various types of personal data about you, including:

- **Identification information:** e.g., full name, gender, place and date of birth, nationality, identity card number, passport number, photograph, signature);
- **Contact information:** (private or professional) postal address, e-mail address, phone number;
- **Information relating to your family situation:** e.g., marital status, number of children and age,
- **Financial and fiscal information:** e.g. salary, other revenues, asset-value, fiscal identification number, tax status, country of residence;
- **Education and employment information:** e.g., level of education, employment, employer's name and remuneration;
- **Banking and financial information related to the products and services you hold:** e.g., payment account details, payment card number, money transfers, domiciliations, data on the beneficiary or principal, payment incidents;
- **Transaction data:** e.g. account movements and balances, transactions including beneficiary's data such as full names, addresses and contact details as well as details of bank transactions, amount, date, time and type of transaction (credit card, transfer, direct debit);
- **Data relating to your habits and preferences in relation to the use of our products and services;**
- **Data collected in the context of your interactions with us, our customer and commercial services, our website, our mobile application, our official pages on social networks:** for example, your comments, suggestions, needs collected during our exchanges with you online during telephone communications (conversation), email discussions, exchanges on our pages on social networks and

your last complaints. Your connection and tracking data such as cookies and tracers for non-advertising or analytical purposes on our websites, our online services, our applications, our pages on social networks;

- **Geolocation data:** e.g., showing locations of withdrawals or payments for security reasons, or to identify the location of the nearest branch or service suppliers for you;
- **Data about your devices (mobile phone, computer, tablet, etc.):** IP address, geolocation, technical specifications and uniquely identifying data;
- **Personalized login credentials or security features** used to connect you to your personal client space on the Nickel website and mobile application.

We may collect sensitive data such as health data, biometric data, or data relating to criminal offences, subject to compliance with the strict conditions set out in data protection regulations.

Indirect collection

We may also collect information about you indirectly even though you are not a Nickel customer, including:

- Identification, contact and digital activity data of prospects;
- Identification and contact data of legal representatives, family members, heirs, debtors (e.g., in the event of bankruptcy proceedings or overindebtedness), corporate officers.

5. From whom do we collect personal data from?

We collect personal data directly from you; however, we may also collect personal data from other sources.

We sometimes collect data from public sources:

- publications/databases made available by official authorities or third parties (e.g., the Journal Officiel de la République Française, the Bulletin Officiel des Annonces Civiles et Commerciales, the Registre du Commerces et des Sociétés);
- websites/social media pages of legal entities or business clients containing information that you have disclosed (e.g., your own website or social media page);
- public information such as that published in the press.

We also collect personal data from third parties:

- from other BNP Paribas Group entities;
- from our customers (companies or individuals);
- from our business partners;
- from service providers of payment initiation and account aggregators (service providers of account information).

6. With whom do we share your personal data?

6.1. With BNP Paribas Group entities

As a member of the BNP Paribas Group, we work closely with the Group's other companies worldwide. Your personal data may therefore be shared between BNP Paribas Group entities, where necessary, to:

- comply with our various legal and regulatory obligations described above;
- fulfil our legitimate interests which are to manage, prevent and detect fraud;
- if you have given your consent, offer you access to all of BNP Paribas Group's products and services that best meet your needs and wishes.

6.2. With recipients outside the BNP Paribas Group and subcontractors

In order to fulfill some of the purposes described in this Privacy Notice, we may, where necessary, share your personal data with:

- processors which perform services on our behalf (e.g., IT services, logistics, printing services, telecommunication, debt collection services, advisory and distribution and marketing);
- banking and business partners, independent agents, intermediaries or brokers, financial institutions, counterparties, banks, correspondent banks, insurance companies, payment system operators, payment card issuers or intermediaries;
- local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, public authorities or institutions (e.g., the Banque de France, Caisse des dépôts et des Consignations), to which we, or any member of the BNP Paribas Group, are required to disclose pursuant to:
 - o at their request;
 - o in connection with our defense, an action or proceeding;
 - o in order to comply with any regulation or recommendation issued by a competent authority with respect to us or any member of the BNP Paribas Group;
- service providers of third-party payment (information on your bank accounts), for the purposes of providing a payment initiation or account information service if you have consented to the transfer of your personal data to that third party;
- certain regulated professions such as lawyers, notaries, or auditors when needed under specific circumstances (litigation, audit, etc.) as well as to our insurers or to an actual or proposed purchaser of the companies or businesses of the BNP Paribas Group.

7. International transfers of personal data

In the case of international transfers from the European Economic Area (EEA) to a country outside the EEA, the transfer of your personal data may take place on the basis of a decision by the European Commission, where the country to which your data will be transferred has been recognized by the Commission as providing an adequate level of protection.

If we transfer your data to a country whose level of protection for your data has not been recognized as adequate by the European Commission, we will either rely on an exemption applicable to the specific situation (for example, if the transfer is necessary to perform a contract with you, such as when making an international payment) 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;
- binding corporate rules.

To obtain a copy of these or to find out how to access them, you may send a written request to the address indicated in Section 10.

8. How long do we store your personal data?

For more information on the retention periods of your data, you can consult **Schedule 2**.

9. How to follow the evolution of this privacy notice?

In a world where technologies are constantly evolving, we regularly review this notice and update it if necessary.

You can find this notice directly on our website (<https://nickel.eu/fr>) in the "Legal documents" section.

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

10. How to contact us?

If you are a Nickel client, you can exercise your right autonomously through your access rights, correction and withdrawal rights on your client space. You can exercise your deletion rights, rights regarding the transfer of data, limitation of usage by sending us an email at donneespersonnelles@nickel.eu.

The following articles of our help center explain how to exercise your rights:

How to request an export of my personal data?

How to modify my personal data (name, surname, email address, phone number, postal address)?

How to limit the treatment of my personal data?

How to delete my personal data?

Schedule 1 - Processing of personal data to combat money laundering and the financing of terrorism

We are part of a banking Group that must adopt and maintain a robust anti-money laundering and countering the financing of terrorism (AML/CFT) programme for all its entities managed at central level, an anti-corruption program, as well as a mechanism to ensure compliance with international Sanctions (this refers to all economic or commercial sanctions, including all laws, regulations, restrictive measures, embargoes or asset restrictions, embargoes or asset freezes, enacted, governed, imposed or enforced by the French Republic the European Union, the US Department of the Treasury's Office of Foreign Asset Control, and any competent authority in the territory where we are established).

In this context, we act as joint controllers together with BNP Paribas SA, the parent company of the BNP Paribas Group (the term "we" used in this appendix therefore also covers BNP Paribas SA).

To comply with AML/CFT obligations and with international Sanctions, we carry out the processing operations listed hereinafter to comply with our legal obligations:

- A Know Your Customer (KYC) program reasonably designed to identify, verify and update the identity of our customers, including where applicable, their respective beneficial owners and proxy holders;
- A Know Your Intermediary (KYI) system for the distribution of Nickel's products and Nickel's products and services, reasonably designed to ensure the integrity and compliance with compliance with legal and regulatory constraints;
- Enhanced due diligence for high-risk clients, Politically Exposed Persons or "PEPs" (PEPs are persons defined by the regulations who, due to their function or position (political, jurisdictional or administrative), are more exposed to these risks, and for situations of increased risk;
- Written policies, procedures and controls reasonably designed to ensure that the Bank does not establish or maintain relationships with shell banks;
- A policy, based on the internal assessment of risks and of the economic situation, to generally not process or otherwise engage, regardless of the currency, in activity or business:
 - for, on behalf of, or for the benefit of any individual, entity or organisation subject to Sanctions by the French Republic, the European Union, the United States, the United Nations, or, in certain cases, other local sanctions in territories where the Group operates;
 - involving directly or indirectly sanctioned territories, including Crimea/Sevastopol, Cuba, Iran, North Korea, or Syria;
 - involving financial institutions or territories which could be connected to or controlled by terrorist organisations, recognised as such by the relevant authorities in France, the European Union, the U.S. or the United Nations.
- Customer database screening and transaction filtering reasonably designed to ensure compliance with applicable laws;
- Systems and processes designed to detect and report suspicious activity to the relevant regulatory authorities;
- A compliance program reasonably designed to prevent and detect bribery and influence peddling in accordance with the Belgian anti-bribery legislative package, the "Sapin II" law, the U.S FCPA, and the UK Bribery Act.

In this context, we make use of:

- services provided by external providers that maintain updated lists of PEPs such as Dow Jones Factiva (provided by Dow Jones & Company, Inc.) and the World-Check service (provided by REFINITIV, REFINITIV US LLC and London Bank of Exchanges);
- public information available in the press on facts related to money laundering, the financing of terrorism or corruption;
- knowledge of a risky behaviour or situation (existence of a suspicious transaction report or equivalent) that can be identified at the BNP Paribas Group level.

We carry out these checks when you enter into a relationship with us, but also throughout the relationship we have with you, both on yourself and on the transactions you carry out. At the end of the relationship and if you have been the subject of an alert, this information will be stored in order to identify you and to adapt our controls if you enter into a new relationship with a BNP Paribas Group entity, or in the context of a transaction to which you are a party.



In order to comply with our legal obligations, we exchange information collected for AML/CFT, anti-corruption or international Sanctions purposes between BNP Paribas Group entities. When your data are exchanged with countries outside the European Economic Area that do not provide an adequate level of protection, the transfers are governed by the European Commission's standard contractual clauses. When additional data are collected and exchanged in order to comply with the regulations of non-EU countries, this processing is necessary for our legitimate interest, which is to enable the BNP Paribas Group and its entities to comply with their legal obligations and to avoid local penalties.

Schedule 2 - Data retention periods

We store your personal data for as long as is necessary to comply with applicable laws and regulations, or for as long as is necessary for our operational constraints, such as accounting, effective customer relationship management, as well as to enforce legal rights or respond to requests from regulatory bodies. For example, most customer data is kept for the duration of the contractual relationship and for 10 years after the end of the latter. As for prospects, this data is stored for 3 years.