Information Notice regarding the protection of personal data

Clients and prospects

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, which operates in Belgium through its Belgian branch whose registered office is located at Rue Royale 144-146, 1000 Brussels and which is registered with the Crossroads Bank for Enterprises under number BE0673.863.661 and with the National Bank of Belgium under number 964 ("**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

Are you subject to this notice? 3

How can you control the processing activities we do on your personal data? **3**
- Right of access 3
- Right to correct 3
- Deletion right 3
- Right to object to the processing of your personal data based on legitimate interests 3
- Right to object to the processing of your personal data for commercial prospecting purposes 3
- Right to suspend the use of your personal data 4
- Rights against an automated decision 4
- Right to withdraw your consent 4
- Right to request the portability of your personal data 4

Why and on which legal basis do we use your personal data? **4**
- To comply with our various legal and regulatory obligations 4
- For anti-money laundering and countering of the financing of terrorism purposes 4
- To perform a contract to which you are a party or pre-contractual measures taken at your request. 5
- To fulfill our legitimate interest or that of a third party 5
  - 3.4.1 In the framework of our business as a payment service provider we use your personal data to : 5
  - 3.4.2 We use your data to perform standard profiling to personalize our products and offers 5
- Respect your choice when you have consented to a specific treatment 6

What type of data do we collect ? **6**

From whom do we collect personal data from ? **7**

With whom do we share your personal data ? **7**
- With BNP Paribas Group entities 7
- With recipients outside the BNP Paribas Group and subcontractors 8

International transfers of personal data **8**

How long do we store your personal data ? **8**

How to follow the evolution of this privacy notice? **8**

How to contact us ? **9**

Schedule 1 - Processing of personal data to combat money laundering and terrorist financing **10**

Schedule 2 - Storage date **12**

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 personaldata@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: personaldata@nickel.eu

In addition to the rights mentioned below, you may lodge a complaint with the DPA (Data Protection Authority).

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 DPA, 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. Rights 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?

L'objectif de cette section est de vous expliquer pourquoi nous traitons vos données personnelles et sur quelle base légale nous nous reposons pour le justifier.

Vos données personnelles sont traitées pour :

3.1. To comply with our various legal and regulatory obligations

Vos données personnelles sont traitées lorsque cela est nécessaire pour nous permettre de respecter les réglementations auxquelles nous sommes soumis, notamment en tant que prestataire de services de paiement.

Nous utilisons vos données personnelles pour :

- 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;
- 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 fulfil 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:
  - we keep evidence of transactions, including in electronic format;
  - Monitor your transactions to manage, prevent and detect fraud;
  - We collect debts;
  - 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 :
  - 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;
  - security: to prevent potential incidents and improve security management;
  - compliance (such as anti-money laundering and anti-terrorist financing) and risk management;
  - 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;
- **Lifestyle**: hobbies and interests, travel, your environment (nomadic, sedentary);
- **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 Official Belgian Gazette, the Crossroads Database for Enterprises);
- 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;
- 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 fulfil 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 National Bank of Belgium, Caisse des dépôts et des Consignations), to which we, or any member of the BNP Paribas Group, are required to disclose pursuant to:
  - at their request;
  - in connection with our defense, an action or proceeding;
  - 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/) 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 personaldata@nickel.eu.

The following articles of our help centre 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 (i.e., any economic or trade sanctions, including associated laws, regulations, restrictive measures, embargoes, and asset freezing measures that are enacted, administered, imposed, or enforced by Belgium, the French Republic, the European Union, the U.S. Department of the Treasury's Office of Foreign Assets Control, and any competent authority in territories where BNP Paribas Group is 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;
- 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 Belgium, 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 Belgium, 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.

Annexe 2 - Durées de conservation

Retention periods' update: December 2024

FIELD OF ACTIVITY	PROCESSING	RETENTION PERIOD
MARKETING & COMMUNICATION		
	Communicate regulatory information to customers (e.g. GTCs, KYC recertification, etc.) and carry out specific transactional communications related to SEPA regulations	Duration of the contractual relationship
	Communication on fraud prevention	Duration of the contractual relationship
	Global information and other transactional communications	Duration of the contractual relationship
	Collect customer and prospect opinions via surveys and telephone interviews about their Nickel experience	3 years from collection for customers and prospects
	Communicate with customers on overall account management, referral campaigns or existing/new products/services/offers to increase customer sales Communicate with prospects or closed customers to guide them through the (re)subscription process	Duration of the contractual relationship (for customers) 3 years from collection (for prospects)
	Send personalized communications to customers based on their usage or consumption habits in order to promote Nickel offers and services	Duration of the contractual relationship
	Communication on our partners' offers and services	Duration of the contractual relationship 1 year from organization
	Manage contests for customers and prospects	1 month from end of competition
	Monitor and moderate social networks to preserve Nickel's brand image	Duration of the contractual relationship
CUSTOMER SERVICE		

	Processing customer requests from social networks via our ZenDesk ticket management tool	Until 5 years
	Processing of external requests with removal of banking secrecy and seizure of the customer's account	All the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Management of special situations and customer account management during the contractual relationship	All the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Managing relations with social and legal bodies	All the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Processing GDPR requests coming from customers in order to meet their needs or support them in their procedures	Telephone records: 3 months ; Legal period: all the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Contacting customers about any KYC inconsistencies identified	Telephone records: 3 months ; Legal period: all the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
	Processing anti-money laundering and terrorist financing alerts	All the individual's identity data and bank details: 5 years from the closing of an account Information relating to operations 5 years from their execution
IT DEPARTMENT		

	Checks, controls and analyses of SEPA flows and accounting disparities to ensure proper execution of transactions and combat fraud	10 years after the date of execution of the operation
	Analysis of customer complaints and customer service requests	10 years after the date of execution of the operation
	Contact with fellow banks to analyze certain requests	10 years after the date of execution of the operation
	Analysis of survey requests received from other banks	10 years after the date of execution of the operation
	Monitoring of accounts and transactions to fight against cyberfraud	Until 5 years
LEGAL		
	Clients' dispute processing by receipting of mails, processing of requests with the support of relevant internal departments, reply by mail to the applicant	Depending on the cases: - 5 years by default - as long as the individual is a Nickel client + legal limitation period in terms of civil liability
	Internal reporting and communication with Group Legal	Until 5 years
ACCOUNTING OBLIGATIONS		
	Analysis of the age of customer accounts receivable to determine provisions or write-offs	10 years from the end of the accounting year
	Access to legal files on customer disputes (FPE) to estimate amounts and prepare accounting documents	10 years from the end of the accounting year
	Collection of required tax data (surname, first name, ID, card, etc.) for all transactions subject to VAT	10 years from the end of the accounting year
	(Except in Portugal and Germany) Regulatory Report	10 years from the end of the accounting year
	(Portugal Only) Tax Reports : Stamp Duty Report (DMIS) / SAFT to PTA / Invoice to the customer	10 years from the end of the accounting year
OTHER OFFERS AND SERVICES		
	Collection of consent to transmit the personal data required to access our RIA partner's offer	Until consent is withdrawn

CUSTOMER DATA MANAGEMENT		
	Data collection, recording, organization, structuring, adaptation, modification, extraction, reconciliation, analysis from internal of partner data sources to make it ready for internal use by the Business Units	Until 10 years
	Deletion or destruction of customer and prospects data based on GDPR requirements	Until 10 years after account closure for customers 3 years for prospects
	Algorithm creation and implementation of machine learning for the purpose of optimizing business lines' and functions' processes	Until 10 years
	Collect data from Nickel's SAAS services to monitor performance and produce follow-up dashboards and reports	Until 10 years
	Storage of cookies data (customers and prospects) based on consent collection to improve functionalities and customer experience. Read the cookies policy for more information: https://nickel.eu/fr/politique-dutilisation-des-cookies	Until 13 months
COMPLIANCE		
	Internal alerts processing through detection of an alert via an algorithm, account analysis, investigation,discussion with the client and collection of client's supporting documents	Belgium : 10 years after the relationship end
	External alerts processing by collecting, verifying and targeting client's concerned personal data.	Belgium : 10 years after the relationship end
	BNPP intra-group exchanges by sending of emails / phone exchanges of our clients personal data , of any type, with other banks in the context of investigations / financial security	Belgium : 10 years after the relationship end d upon expiry of a period of 10 years at the latest.

	Information transfer with third-parties / institutions in the context of investigations (outside BNPP group)	Belgium : 10 years after the relationship end
	External exchanges by sending of the summary sheet (KYC Flux + supporting documents) along with an investigation report	Belgium : 10 years after the relationship end
	Compliance Permanent Control : review of alerts treatment by Compliance acting	Belgium : 10 years after the relationship end
	Complaints handling by receiving and processing customer complaints in order to provide an appropriate response within a reasonable timeframe	Belgium : 10 years after the relationship end
	Use of the Call for vigilance lists in screening algos and conservation of the list 6 months after the end of the vigilance call	Belgium : 10 years after the relationship end
	Transmission of fraudsters' data (description of the data management)	Belgium : 10 years after the relationship end
FRAUD AND REGULATORY		
	Fraud management: internal and external investigations and monitoring by collection and cross-checking of the data about suffered fraud or committed fraud of our customers	Until 5 years
	Regulatory projects : by collecting and cross checking the data in order to steer regulatory projects	Until 10 years
	Regulatory reporting to local regulation authorities (OTESI, ATRUVIA…)	10 to 30 years (depend on the applicable local regulation)
PAYMENT ACTIVITY		
	Wallet Enrolment for Apple	Until 7 years

	Wallet Enrolment for Google	Until 7 years
	Wallet Enrolment for Mastercard for Merchants, Click to Pay	Until 7 years
	Regular checking of walllet eligibility and display of information for all wallets	Duration of the contractual relationship
	Card Management (ordering, offer, lifecycle, PIN...)	Until 10 years (except card lifecycle: 7 years)
	Management of the card insurance	Until 10 years
	Card Payment Management	Until 10 years
	SEPA Management (Direct Debit Management, Credit Transfer Management, Instant Transfer Management)	Until 10 years
	Top Up Management : process to credit the Nickel account using another bank credit card	Until 10 years
	Rewards Management by rewarding clients/tobacconist that did great results by boosting their commission rates or giving them one time bonuses	Until 10 years
	Internal process to perform payment, withdrawal and deposit using the Nickel POS	Until 10 years
	Having fraud rules implemented on the payment system based on risk analysis to refuse transaction	Until 10 years
	Bank Account Management through account creation for customer, manage the accounting flow, manage the lifecycle of an account	Until 10 years
	Payment Limit Management : defines the payment limits per customer, the pricing and fees	Until 10 years
	Pricing & Fees Management by defining the pricing for each products and services and through planification, fee taking, cancellation, refund	Until 10 years
	Tax Management by managing the applicable taxes specific to Portuguese regulatory	Until 10 years
CUSTOMER EXPERIENCE		
	Customer authentication for validation of sensitive transactions	Until 10 years
	Operations management by displaying user interface operations	Until 5 years

	KYC management by displaying KYC on user interfaces and processing KYC	Until 10 years
	Displaying card data on user interfaces	Until 10 years (except card lifecycle: 7 years)
	Executing transactions on user interfaces	Until 5 years
	Communication management for customers	Duration of the contractual relationship
	Handling any type of customer request	Until 5 years except for telephone records: 3 months
CUSTOMER ACQUISITION		
	Acquisition of new customers through a full online process	Duration of the contractual relationship
	Management of customer acquisition through the use of advertising platforms	3 years from collection
	Management of customer acquisition through the use of affiliation platform	3 years from collection
	Sending hashed email to Google Ads to improve conversions and enrich algorithms (enhanced conversion)	20 days
	Management of customer acquisition and budget allocation through the use of advertising platforms Retargeting of Nickel website visitors to send personalised communication to prospects (current test)	3 to 6 months for cookie storage
	Enhancement of the current acquisition framework by testing the solution of several external providers	Until the end of the test
	Biometric consistency check at the time the relationship is established by analysing and comparing identity documents	Duration of the contractual relationship