INFORMATION ON THE PROCESSING OF PERSONAL DATA

The purpose of this information notice is to inform you in a transparent manner about the processing that we may implement throughout the banking relationship, with regard to our customers, prospects or natural persons involved in a relationship with a customer such as an agent, legal representative, guarantor, designated contact, employee or beneficial owner, etc.

1. WHO COLLECTS YOUR PERSONAL DATA

You use our Caisse d'Epargne services on a daily basis and you know us well. We support you through our network of branches, our employees, the remote services made available to you and, where applicable, through our agents and distributors.

As the hub of this banking relationship, we are in charge of the collection and processing of personal data related to this main relationship. In this respect, we act as DATA CONTROLLER.

To provide these services and offer you a variety of products designed to meet your needs, we are not alone. We are part of a wider group of companies, the BPCE Group and enter into partnerships with companies.

All of these companies contribute to the services provided to you or distributed through us and ensure compliance with the same principles. They may be provided with your personal data for this purpose.

For example:

You may subscribe to products or services marketed by us as an intermediary but which are supplied by another company.

In that case, you establish a direct contractual relationship with the partner concerned. Depending on the product or service subscribed, we will act either as a distributor (the contract will be drawn up and subscribed through us in our capacity as representative of the partner), or in our capacity as a business introducer (you will enter into the contract directly with the partner to whom we have introduced you).

In these situations, your personal data will be collected and processed by us as a distributor or introducer and the partner, each as far as it is concerned and each for the specific purposes related to the products and services subscribed to.

The information applicable to the protection of personal data relating to a product subscribed to with a partner is communicated to you by that partner, in the capacity of DATA CONTROLLER for the collection and processing that it implements on its own behalf.

If you wish to obtain additional information on BPCE Group companies and their various business lines: www.groupebpce.fr.

2. HOW WE OBTAIN YOUR PERSONAL DATA

In the course of our banking relationship, we will collect and process personal data about you. That data may vary depending on the nature of the product or service subscribed.

PERSONAL DATA AND INFORMATION YOU PROVIDE TO US

When entering into a relationship, then when taking out any new product or service (account, credit, savings, insurance, ancillary services, etc.), we collect the data necessary for that transaction directly from you.

This data is necessary:

- to enable us to fulfil our legal and regulatory obligations, such as the obligation to know our customer, our tax obligations or relating to the fight against money laundering and the financing of terrorism,
- to know you, advise you and offer you the range of products and services that meet your needs,
- for subscription of the product or service concerned,
- for its operation.

As such, you provide us with personal data relating to your identity, family situation, professional life and, more generally, your economic, tax, asset and financial situation.

You also provide us with your contact data, including your email and mobile phone number so that we can send you information in connection with provision of the service, send notifications such as those relating to management of your digital contracts and documents or to complete banking transactions, as well as, with your consent, to send you marketing information (email, SMS, MMS).

Certain personal data may be collected for regulatory or contractual purposes or because it is required to conclude a contract. You are informed, where applicable, of the consequences of a refusal to communicate.

For example, your refusal to:

- provide us with mandatory data for the opening and management of an account would prevent us from proceeding with that opening,
- provide us with information relating to your financial situation would prevent us from considering your loan application,
- provide us with the information necessary to analyse your situation and your needs could prevent us from providing you with appropriate advice.

Some data may also be collected:

- when you participate in competitions organised by us,
- when you perform simulations on our websites, request information or ask for contact.

PERSONAL DATA FROM THE USE OF THE BANK'S PRODUCTS AND SERVICES

When you use our products and services or carry out transactions and operations, personal data is processed in our information systems.

PERSONAL DATA FROM THIRD PARTIES OR OTHER SERVICES

Personal data may also come from:

- third-party suppliers, subcontractors such as Carte Bancaire, Visa or Mastercard,
- partners of the Bank if their personal data protection policies allow,
- other products or services provided by third parties to which you have subscribed and for which you authorise sharing with the Bank,
- records that the Bank must consult to provide certain services, under specified regulatory conditions, such as the French national consumer credit files (FICP – *Fichier National des Incidents de Remboursement des Crédits aux Particuliers*) maintained by the Banque de France or the French centralised cheque file (FCC – *Fichier Central des Chèques*).

PUBLIC PERSONAL DATA

We may collect public personal information about you.

Public personal data is personal information or data produced or received by an administrative authority within the framework of its public service mission, published by an administrative authority or able to be communicated to anybody upon request.

We may use public personal information or data when authorised by laws or regulations and in accordance with the specific rules of communication and re-use specified by said texts.

PERSONAL DATA ENRICHED BY THE BANK

Based on personal data collected for reporting or operational purposes, we can generate or calculate new personal data.

This is particularly the case during a credit application when we analyse your request and calculate a credit rating or when, in accordance with our legal and regulatory obligations, we determine credit risk, fraud risk or any other assessment.

In addition, we define profiles and customer segments in order to know our customers, adapt our products and services or customise offers made to you.

EXCLUSION OF SPECIAL CATEGORIES OF PERSONAL DATA

Special categories of personal data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, personal data concerning health or personal data concerning a natural person's sex life or sexual orientation.

As a matter of principle, we do not collect or process any of these special categories of personal data.

However, some of this data may be collected and processed in specific situations. For example:

- For the implementation of a strong authentication system allowing you to access your online banking services, make a payment or sign electronically, using biometric recognition systems (voice recognition, facial recognition, fingerprints, etc.). The use of this data makes it possible to prevent fraud and theft of your identity by a third party. These biometric

recognition systems are an alternative to other control mechanisms and are subject to specific security measures to ensure the security and confidentiality of personal data.

- When taking out a personal insurance policy, such as borrower insurance. In this case, the insurer may need information relating to your state of health to grant you its cover and set any exclusions. The procedures implemented aim to ensure full compliance with the principle of partitioning: only the insurer will receive this data and will process it according to the rules specific to it in compliance with applicable regulations, whereas the bank will only be aware of the approval or rejection decision.

In any event, if we have to process these special categories of personal data, provided that it is not prohibited by applicable law or regulation, your consent will be collected beforehand.

3. WHO ACCESSES YOUR DATA

As a banking institution, we are bound by professional secrecy and may only share your data under strict conditions or with your consent.

The same principle of secrecy and confidentiality applies to all stakeholders involved, whether they are our employees, service providers, partners or their own employees.

Within the BPCE Group, we may need to disclose your personal data to the following entities:

- to BPCE S.A. acting as central body of the BPCE Group so that it can fulfil the various tasks assigned to it by law, for the benefit of our establishment and the Group, for the benefit of Reference and the Group, particularly in terms of prudential reporting to any competent regulatory authority or for the purposes of managing data governance on behalf of BPCE Group establishments.

  Data governance refers to the organisation and procedures put in place to supervise data collection and usage practices within the BPCE Group and to optimise the effectiveness of the use of this data in accordance with the legal and ethical framework.
- Any BPCE Group entity for the power to offer you products or services managed by such entities.
- Entities belonging to our group (BPCE, Banques Populaires/Caisses d'Epargne, Natixis Assurance, Natixis Financement, Natixis Lease, etc.) for the study or preparation of all types of contracts or transactions concerning you.
- Any BPCE Group entity with which you enter or have entered into a contractual relationship for the purpose of updating data relating to your civil status, family, wealth and financial situation, the operation of your account or the rating assigned to you for the application of banking regulations, collected by those entities, including information relating to your tax status. This data may also be used for the review of your file, the use of products and/or services subscribed or their recovery.
- BPCE Group entities or service providers, in the event of the pooling of technical resources, particularly IT resources on behalf of our establishment. For this purpose, your personal data may be pseudonymised for the purpose of researching and creating statistical models. Pseudonymisation means that the data in question will no longer be linked to your person without the use of additional information,

  kept separately and subject to technical and organisational measures to ensure that the initial data can no longer be attributed to an identified or identifiable natural person.

With third parties, we may share your data in the following cases:

- with the companies that secure or guarantee your loans (e.g. insurance companies, mutual guarantee companies),
- with companies whose loans we distribute (e.g. consumer credit); with credit institutions and more generally with the institutions authorised to provide payment services, as well as with the Banque de France, the payment card schemes whose brands appear on your card (e.g. CB, Visa, Mastercard, etc.), merchants or service providers accepting credit cards, for the purposes related to bank cards and payment instruments,
- with recovery companies acting on our behalf,
- with third parties (service providers, subcontractors, etc.) with a view to entrusting them with operational functions (e.g. alerts regarding use of overdraft authorisations, use of mobile payment solutions, management of bank cards or production of chequebooks),
- with third-party companies in the event of assignment of receivables or securitisation transactions,
- to partners of the banking institution, to enable you to benefit from the advantages of a partnership which you have previously decided to join, within the exclusive framework of the partnership agreements, and to enable Groupe BPCE to ensure the monitoring and commercial management of the partnership.
- in the context of competitions, with the bailiffs responsible for monitoring and managing the competition,
- with our banking intermediaries,
- to subcontractors and service providers for the sole purpose of providing services on our behalf and in particular supplying banking and financial products, conducting surveys or compiling statistics.

We share your personal data in the following cases:

- when provided for in this notice,
- when necessary to provide you with products and services subscribed,
- when you consent to such sharing.

We must also share your data when professional secrecy is lifted by law, particularly with regard to tax and customs authorities, the Banque de France (e.g. FCC, FICP), social security bodies (under the conditions provided for in Articles L. 114-19 to L. 114-21 of the French Social Security Code), the French Prudential Supervisory and Resolution Authority (ACPR – *Autorité de Contrôle Prudentiel et de Résolution*) and parliamentary investigation committees. Secrecy is also lifted with regard to the information required for the application of agreements concluded by France, organising an automatic exchange of information for tax purposes (Article 1649 AC of the French General Tax Code). Secrecy cannot be enforced on the judicial authority acting within the framework of criminal proceedings or as part of civil proceedings when a specific text expressly provides for it.

4. WHY WE PROCESS YOUR PERSONAL DATA

As part of our banking relationship, we use all or part of the personal data about you for the purposes described below and based on the following grounds:

TO PERFORM THE CONTRACT RELATING TO THE PRODUCTS AND SERVICES YOU HAVE SUBSCRIBED TO OR THAT YOU WISH TO SUBSCRIBE TO

We process your personal data first and foremost in order to provide the products and services you subscribe to, or that you wish to subscribe to.

Processing is carried out because it is necessary for performance of the contract or for the performance of pre-contractual measures taken at your request as a customer, in the context of an already established relationship, or as a prospect if no business relationship has yet been established (pre-contractual measures such as the provision of advice, a proposal or a simulation).

The processing carried out in the context of the management of our relationship concerns, in particular, the maintenance of your bank accounts and performance of transactions, the management of your banking and savings products, the manufacture of your payment instruments such as your bank card, as well as the management of their operation and the security of payment transactions, particularly when the payment instrument is the subject of an objection (or blocking), granting and managing your loans, issuing or obtaining guarantees, issuing or obtaining guarantees, preventing and managing unpaid amounts and over-indebtedness, managing insurance policies, collecting and managing litigation.

Without such processing, we would not be able to conclude or perform the contract.

Prior to the authorisation of a payment transaction, we may implement automated decision-making based in particular on analysis of payment instrument information, the context of the transaction, the balance of the account on which the payment instrument operates and the ceilings for its use. Automated decision-making may result in authorisation or refusal of the payment transaction.

TO MEET OUR LEGAL AND REGULATORY OBLIGATIONS

We operate in a very strict regulatory environment, whether it involves carrying out banking transactions or related transactions, distributing insurance products or other intermediation operations.

To meet these legal obligations, we process personal data.

As a result, we may need to request specific information about certain transactions if required by law or regulations.

Automatic exchange of information in tax matters.
We are required to identify, for tax purposes, the residence of the account holder and to fulfil the obligations of annual reporting to the French tax authorities relating to reportable accounts of persons who are non-tax resident in France (including specified US Persons, within the meaning of FATCA).

The French tax authorities shall pass on this information to the tax authorities of the declarable account holder's country of tax residence if required by the regulations concerning the automatic exchange of information.

Anti-money laundering and combating the financing of terrorism.
We are required to identify our customers and, where applicable, the beneficial owners of the transactions and are bound by an obligation of constant vigilance with regard to our customers throughout the duration of the business relationship (amount and nature of the transactions, source and destination of the funds, monitoring of the professional, economic and financial situation of the customer, etc.). The information you provide to us must therefore be regularly updated.

As such, we are required to apply special due diligence measures with respect to Politically Exposed Persons defined by the French Monetary and Financial Code.

We are also required to report certain transactions to the relevant authorities, in particular:

- sums recorded in our books and transactions relating to sums that may come from an offence punishable by a custodial sentence or that could contribute to the financing of terrorism,
- transactions for which the identity of the instructing party or beneficial owner of the transaction remains doubtful despite the due diligence carried out under the identity verification obligation incumbent on the Bank.

INFORMATION NEEDED TO MAINTAIN REGULATORY FILES

By way of example, we disclose the personal data necessary to maintain the following regulatory files, which we may also be required to consult:

- **FCC.** The French centralised cheque file (*Fichier Central des Chèques*) lists the personal data which Banks are required to provide concerning the identity of persons who have issued a dishonoured cheque and the identity of the persons to whom a prohibition applies for another reason (e.g. certain joint-account holders).
- **Central file of CB bank-card withdrawals. This** file, managed by the Banque de France, identifies decisions to withdraw a CB card when a payment incident resulting directly from the use of the CB card has not been resolved.
- **FICOBA.** When opening a bank account or similar account for a customer, banks are required to declare a certain amount of information to the French Directorate General of Public Finance in charge of the Bank Accounts File (FICOBA – *Fichier des Comptes Bancaires*) and to inform it of any changes or closure of the account for a period of 10 years after the closure of the account.
- **FICP.** Banks are obliged to report to the French national consumer credit files (*Fichier National des Incidents de Remboursement des Crédits aux Particuliers*) incidents relating to loans granted to natural persons for non-professional purposes. They also have an obligation to consult this file in certain cases (granting credit, overdraft authorisations repayable within a period greater than one month, annual renewal of a revolving credit agreement). It may also be consulted at the time a means of payment is allocated or at the time of the allocation or renewal of a payment card.

Our insurer partners have similar obligations, particularly for declarations regarding entries in the register of capitalisation and life insurance policies (FICOVIE – *fichier des contrats de capitalisation et d'assurance vie*).

OTHER REGULATORY OBLIGATIONS

Vulnerable customers. We have the obligation to identify actual situations of financially vulnerable customers or customers with a "right to an account" in order to contact them and to offer them suitable specific offers.

We must also anticipate situations in which Customers may potentially encounter difficulties in order to take appropriate and personalised measures in response to these difficulties.

Dormant accounts. Regulations require banks to record inactive accounts held with them each year. We must therefore consult the French national individual identification register (RNIPP – *Répertoire National d'Identification des Personnes Physiques*) each year for inactive accounts in order to check whether the customer(s) concerned may have died. Similar obligations apply to inactive safe deposit boxes and, for insurers, life insurance policies.

Responses to requests to exercise rights under personal data protection regulations. The exercise of your rights referred to in Article 12 of this document requires the processing of personal data concerning you for the purposes of identifying, managing your requests and retaining evidence.

TO MEET OUR LEGITIMATE INTERESTS

We may invoke a "legitimate interest" in processing your data, particularly when faced with situations that may pose risks to our business such as protecting against market abuse or insider trading, preventing fraud, particularly involving payment instruments, and managing any legal remedies, combating financial crime, both with regard to the financial sector and in respect of our customers and employees, preventing and managing rudeness to our employees, ensuring the security of our networks and information, and monitoring access to our premises, particularly via a video surveillance system.

This legitimate interest may be linked to the analysis of our commitment risk, in particular during assessment of risks related to credit applications and throughout the contractual relationship. The automated processing carried out within this framework ultimately includes human intervention and leads to a decision to grant or refuse credit. You have the right to comment and challenge the decision taken at the end of this process.

Our legitimate interest may also be linked to the management of our business as a company (general accounting, invoicing, balance sheet management, reporting, statistical studies and satisfaction surveys), the management of our customer relationship (improvement of customer knowledge, improvement of our products and services, monitoring, design, development and monitoring of commercial activity including within the framework of commercial offers proposed by our partners), prospecting, profiling and marketing segmentation, including combining data for analysis or anonymisation purposes, where relevant, or for our audit, inspection and communication activities.

These processing operations are implemented in accordance with your interests and fundamental rights. As such, they are accompanied by measures and guarantees to ensure a balance between the protection of your interests and rights and the pursuit of our legitimate interests.

TO IMPLEMENT CERTAIN PROCESSING OPERATIONS WITH YOUR CONSENT

We may carry out processing when you have consented to it for one or more specific purposes.

In that case, you will first be asked to give your consent, specifically, to the collection and processing of your data for one or more identified purposes.

When we wish to carry out commercial prospecting by email, for instance, we obtain your consent prior to sending our commercial offers.

5. HOW LONG YOUR DATA IS RETAINED

Once the purposes of processing the data have been achieved, and subject to any legal or regulatory obligations requiring the retention of certain data, we will delete or anonymise your data.

The retention period varies and depends on the nature of the data and the purposes pursued.

Personal data collected for the purposes of managing a contract: the data is retained for the time necessary for performance of the contract and until expiry of the applicable legal periods.

These time periods are of several types:

- in accordance with the provisions of the French Commercial Code, accounting documents and supporting documents must be retained for a period of **10 years.** Personal data necessary for performance of this obligation will therefore be retained for that period. The 10-year period generally runs from the date of the transaction. For example, for a transaction recorded on your bank account, the data retention period relating to that transaction will be 10 years from its date,
- the limitation period under ordinary law in civil and commercial matters is five years. For example, the data relating to your account will be retained for a period of five years from the closure of your account or the termination of our relationship,
- the time periods corresponding to specific legislation, such as anti-money laundering and combating the financing of terrorism legislation, are five years,
- the time period necessary for the purpose in question, such as combating fraud, for example, which is five years.

These time periods may be longer in certain specific situations, when required by regulations, for example for the management of dormant accounts, in order to comply with tax provisions (particularly relating to regulated savings). They may also be longer in the event of legal proceedings. In that case, the data is retained until the end of the legal proceedings and then archived according to the applicable statutory limitation periods.

When personal data is collected for several purposes, it is kept until expiry of the longest retention or archiving period.

After termination of the relationship, we may also retain your data and use some of this information (your name, address, date and place of birth, characteristics of the product previously subscribed) for commercial prospecting purposes for a maximum period of five years (from the last incoming contact). You may object at any time to processing for commercial prospecting purposes, under the conditions provided for in Article 12 hereof.

PERSONAL DATA COLLECTED FOR PRE-CONTRACTUAL PURPOSES, WITHOUT EFFECTIVE CONCLUSION OF A CONTRACT

When you have contacted us to request a product, service or simulation and your request has not been followed by a subscription, we retain your data for a period limited to the initial purpose (e.g. to be able to reissue a simulation or trace advice we have provided you).

Where you have made a loan application that resulted in an offer being issued which is ultimately not accepted by you, we retain the data relating to it until expiry of the statutory limitation period.

Where applicable, the result of the lending risk analysis process is retained for a period of six months from the application date.

PERSONAL DATA RELATING TO A NON-CUSTOMER PROSPECT

Personal data relating to a non-customer prospect is retained, for commercial prospecting purposes, for a maximum period of three years from the last contact by the prospect.

That data is also retained for a period of five years for the purposes of combating money laundering and the financing of terrorism and the fight against fraud.

6. HOW WE ENSURE THE SECURITY AND CONFIDENTIALITY OF YOUR DATA

Our priority is the respect of privacy and banking secrecy, the security and confidentiality of data and, in particular, the personal data entrusted by our customers.

In view of the nature of the personal data and the risks presented by its processing, we take the technical and organisational measures necessary to preserve the security of your data and, in particular, to prevent it from being distorted, damaged or accessed by unauthorised third parties and to prevent improper use.

We therefore undertake to take the necessary physical, technical and organisational security measures to:

- maintain the security of our customers' personal data against unauthorized access, alteration, distortion, disclosure or destruction of the personal data we hold,
- protect our business.

We conduct regular internal audits to ensure the security of the personal information and to protect against unauthorised access to our systems.

However, the security and confidentiality of personal data relies on best practices being followed by everyone, so you are advised to be vigilant.

In order to protect the confidentiality of your personal data, we invite you to take all relevant measures, particularly in respect of rules for use of the internet, by deleting browsing data at the end of your browser session and by prohibiting unauthorised access by third parties in the event that you download that data to management software. We invite you to consult the security advice made available to you, particularly via our website.

In accordance with our commitments, we select our subcontractors and service providers with care and impose the following commitments on them:

- a level of protection of personal data equivalent to ours,
- access to and use of personal data or information strictly limited to what is necessary for the services to be provided by them,
- strict compliance with the laws and regulations applicable to confidentiality, banking secrecy and personal data,
- implementation of all appropriate measures to ensure protection of the personal data that they may be required to process,
- definition of the technical and organisational measures necessary to ensure security of the data.

We undertake to enter into contracts with our subcontractors, in accordance with legal and regulatory obligations, precisely defining the terms and conditions for processing the personal data.

7. WHERE YOUR DATA IS STORED

Personal data and information relating to our customers are stored in our information systems or those of our subcontractors or service providers.

We undertake to choose subcontractors and service providers that meet the quality and security criteria and which provide sufficient guarantees, particularly in terms of specialist knowledge, reliability and resources, for the implementation of technical and organisational measures, including in terms of processing security.

As such, we impose confidentiality rules on our subcontractors and service providers that are at least equivalent to our own.

As a matter of principle, we favour technical solutions and the storage of personal data in hosting centres located within the European Union. If this is not the case, we take the necessary measures to ensure that the subcontractors and service providers provide appropriate security and protection measures as described below.

IS YOUR DATA COMMUNICATED OR ACCESSIBLE FROM A COUNTRY OUTSIDE THE EUROPEAN UNION?

Your personal data transmitted in accordance with the agreed purposes may, in the context of various operations, be transferred to a country of the European Union or outside the European Union.

As part of a possible transfer to a country outside the European Union, rules have been put in place to ensure the protection and security of that information.

For these same reasons, in the event of a funds transfer, certain personal data must be transmitted to the transfer beneficiary's bank located in a country of the European Union or outside the European Union.

Such personal data may be communicated, on request, to official bodies and authorised administrative or judicial authorities, or to third parties.

Personal information or data may potentially be transferred outside the Bank's country and/or to non-member countries of the European Union and may be subject to laws or regulations different from those applicable in the European Union.

For example, certain personal data may be hosted in the United States when the Bank executes certain transactions such as transfers through the secure network of the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

In all cases, we take necessary and appropriate measures to ensure banking secrecy and the security of personal data.

To secure transfers of information or personal data outside the European Union, which are not necessary for performance of the transaction or the contract between us or implementation of pre-contractual measures taken at your request, we may, for example, implement standard clauses governing flows defined by the European Commission.

8. OUR PROSPECTING ACTIONS

We may contact you to offer you new products and services that appear to correspond to your needs or desires or meet new uses.

You may object at any time and at no cost to processing for prospecting purposes, in accordance with the terms and conditions defined in Article 12 hereof.

COMMERCIAL PROSPECTING BY EMAIL AND AUTOMATED CALLING

We may prospect you by email, automated calling or SMS when you have given your consent at the time your email address or personal contact details were collected.

Each commercial prospecting email contains a link to unsubscribe.

Messages and notifications related to the administrative management of a previously subscribed product or service (alerts, notifications of the provision of an electronic document on your remote banking space, etc.) do not correspond to commercial prospecting. Such messages and notifications may be configured as part of the subscribed service, it being understood that some of those notifications may be subject to regulatory obligations and are of an imperative nature.

TELEPHONE PROSPECTING

We may also prospect you by telephone.

In accordance with Article L. 223-2 of the French Consumer Code, you are informed that you may register yourself on a "Bloctel" telephone marketing black list. However, despite that registration, we may contact you by telephone if ongoing contractual relations exist between us, unless you have objected or unless you object during the call.

9. OUR PROFILING ACTIONS

Profiling involves using personal data to evaluate certain aspects of the data subject, analyse or predict his/her interests, behaviour or other attributes.

As part of our relationship, we may have to implement two categories of profiling:

- marketing profiling that does not produce legal effects on you, such as marketing segmentation to suggest innovative products and services that may match your expectations/needs, complementary or promotional offers with the best targeting of your needs,
- profiling that may have legal effects on you and lead to a decision such as a credit rating.

Regarding marketing profiling, the Bank uses techniques to carry out segmentation and select marketing targets that do not produce legal effects.

As such, the personal data we collect also helps us to personalise and continuously improve the banking relationship and business relationship in order to offer you the products and services most suited to your needs. We use various profiling techniques for this (including the use of algorithms).

You have the right to object at any time to the processing of your personal data for commercial prospecting purposes.

We may also need to aggregate and anonymise this data to produce marketing reports and models.

When using such techniques, we take the necessary measures to limit the risks of error and breaches of individuals' fundamental rights and freedoms.

In the event that this profiling has legal consequences for you, such as in the event of use of risk assessment processing for credit scoring, the results of the use of these techniques will only be an aid to the Bank's decision-making:

- the Bank's decision-making process always includes human intervention,
- and you have the right to present your comments to us, to obtain an explanation for the decision reached following this type of assessment and to challenge the decision.

10. IMPLEMENTATION OF SPECIAL PROCESSING BASED ON SPECIFIC TECHNOLOGY

VIDEO-PROTECTION

As part of implementation of security measures by our branches and premises, we use video-protection systems in accordance with the rules provided for in the French Internal Security Code and particularly authorisations issued by the competent prefectures and personal data protection regulations.

You are hereby informed that these images are recorded and stored and that they may lead to identification of the persons filmed, either by the systems in use or by agents with access to the images.

Signs in the filmed locations indicate the existence of this type of device, the identity of the data controller and the procedures for exercising your rights of access to the visual recordings concerning you.

The images are retained for a period of one month, except in the case of criminal proceedings. If such proceedings are initiated, the images are then extracted from the device (after recording this operation in a specific log) and retained for the duration of the proceedings.

COOKIES AND OTHER TRACKERS

Cookies and other trackers mean trackers deposited and read, for example, when viewing a website, reading an email, or installing or using software or a mobile app, regardless of the type of terminal used.

You are informed that when you visit one of our sites, cookies and trackers may be installed on your terminal equipment. You may consult the cookies policy in place for the site concerned. Where necessary, we obtain your consent prior to installation of such trackers on your terminal equipment, as well as when we access data stored on your equipment.

The lifespan of these trackers is 13 months maximum.

TELEPHONE RECORDING

Telephone conversations between you and our teams may be subject to telephone recordings for the purpose of training, evaluation or improving the quality of products and services or as evidence of a transaction carried out remotely.

We inform you of this prior to carrying out recording.

The recording media or any copies of them shall be retained for periods proportionate to the purpose of the recording in question.

11. YOUR RIGHTS

Within the limits and conditions authorised by the regulations in force, you may:

- **access** all of your personal data,
- have your personal data **rectified, updated and erased**, it being specified that erasure may only take place when:
  - the personal data is no longer necessary in respect of the purposes for which it was collected or otherwise processed,
  - you have withdrawn your consent, on which the processing was based,
  - you have objected to the processing of your data and there is no compelling legitimate reason for continuing it,
  - the personal data has been processed unlawfully,
  - the personal data must be erased in order to comply with a legal obligation which is provided for by European Union or French law to which the Bank is subject,
- **object** to the processing of your personal data for reasons specific to you,
- **object** to the processing of your personal data for commercial marketing purposes,
- **receive** personal data about you, which you have provided to us for automated processing based on your consent or on the performance of a contract, and request the portability of said data,
- **request limitation** of the processing of personal data we hold about you when:
  - you dispute the accuracy of the personal data, during a time-frame enabling the data controller to verify the accuracy of the personal data,
  - you object to the erasure of data concerning you when its processing is unlawful,
  - we no longer need the data but it is still necessary for the establishment, exercise or defence of legal claims,
  - you have objected to the processing of your data, during verification of whether the legitimate reasons pursued by the Bank override your own,
- where the processing is based on your consent, **withdraw that consent at any time,**
- **lodge a complaint** with a supervisory authority. In France, the supervisory authority is:
  CNIL - 3 Place de Fontenoy - TSA 80715 - 75334 PARIS CEDEX 07 - www.cnil.fr

In addition, you may provide us with instructions relating to the retention, erasure and communication of your data after your death, instructions which may also be registered with "a digital trusted third party". Those instructions may designate an individual responsible for their execution. However, these rights may not have the effect of violating the rights of heirs or allowing the communication of information to which only said heirs may legitimately have access.

12. HOW TO EXERCISE YOUR RIGHTS

If you would like to know more about the provisions of this information notice or contact our Data Protection Officer, you may write to us at the following address: ***Postal address***:

Caisse d'Epargne Hauts de France
Customer Relations Department
Personal Data Protection Officer
8 Rue Vadé
80064 Amiens Cedex 9

email:
delegue-protection-donnees@hdf.caisse-epargne.fr

You can exercise your rights by writing to the following address: ***Postal address:***

Caisse d'Epargne Hauts de France
Customer Relations Department
8 Rue Vadé
80064 Amiens Cedex 9

email: service.client@hdf.caisse-epargne.fr

You must provide proof of your identity by clearly indicating your full name, the address to which you wish the response to be sent to you, signing your request and attaching a photocopy of an identity document bearing your signature.
The exercise of your rights of access, rectification, objection, erasure, restriction of processing or portability of personal data is carried out at no cost.
In respect of exercise of the access right, we will provide you with a copy of the personal data processed. In the event of manifestly unfounded or excessive requests, particularly in respect of their repetitive nature, we may require the payment of reasonable fees to cover the administrative costs incurred in providing such information, communicating with you or taking the requested measures, or else refuse to respond to your request.

This information notice is subject to change. The latest version in force can be consulted at the following address:
https://www.caisse-epargne.fr/da/file/fre-NF/360030

Caisse d'Epargne et de Prévoyance Hauts de France - Cooperative Bank governed by Articles L.512-85 et seq. of the French Monetary and Financial Code - French public limited company (Société Anonyme) with a Management Board and a Steering and Supervisory Committee - Share capital of €1,000,000,000 - Registered office: 612 rue de la Chaude Rivière 59800 LILLE – 383 000 692 RCS Lille Métropole - NAF Code 6419 Z - Intra- Community VAT no. FR34383000692 - Insurance Intermediary registered with ORIAS under number 07 008 031 - Holder of the professional card "Property and business transactions without receipt of funds, bills or securities" no. CPI 8001 2016 000 009 207 issued by the CCI Grand Lille - Financial guarantee: CEGC, 59 avenue Pierre Mendès France, 75013 PARIS.