

INFORMATION ON THE PROCESSING OF PERSONAL DATA

This information sheet is intended to inform you in a transparent way about processes we are likely to implement throughout the banking relationship, related to our customers, prospects or natural persons intervening in the context of a relationship with a client such as a proxy, a legal representative, a guarantor, a designated contact, an attendant or an actual beneficiary...

1. Who collects your personal data
2. How do we gather personal data about you ?
3. Who has access to your data ?
4. Why are we processing your personal data ?
5. How long are your personal data kept ?
6. How do we ensure the security and confidentiality of your data ?
7. Where is your data stored ?
8. Our prospecting actions
9. Implementation of specific processing based on a specific technology
10. Your rights
11. How to exercise your rights

1. WHO COLLECTS YOUR PERSONAL DATA ?

You use services of the payment institution, BIC BRED, daily and you know us well. We support you through our sales representative, our staff, and remote services available to you.

Central player of this banking relationship, we are in charge of the collection and processing of personal data related to this main relationship. We act as the **Data Controller**.

For these services to be available and to offer you a variety of products that meet your needs, we are not alone. We are part of a larger group of companies, the BPCE Group, and we are forming partnerships with companies.

All of these companies contribute to the services provided to you or distributed through us and they ensure that the same principles are ensured.

To do this, they are likely to have access to your personal data.

For example:

You may be asked to subscribe through us products or services that we market but that come from another company.

In this case, you establish a direct contractual relationship with the partner concerned. Depending on the product or service subscribed, we will intervene either as a distributor (the contract will be established and

subscribed through us in our capacity as representative of the partner), or as indicator or contributor (you will subscribe the contract directly with the partner with whom we will put you in contact).

In these situations, your personal data will be collected and processed by us as a distributor or contributor and by the partner, only the one, only when necessary and only with data necessary for the specific purpose related to the process of the subscribed products and services.

The information applicable to the protection of personal data related to a product purchased from a partner are communicated by the latter, as Data Controller for the collection and processing that it implements for its own account.

If you wish to obtain additional information on the BPCE Group member companies and their various businesses : www.groupebpce.fr

2. HOW DO WE OBTAIN PERSONAL DATA ABOUT YOU?

During our relationship, we will collect and process personal data about you. These data can vary according to the nature of the product or service subscribed.

Personal data and information that you communicate to us

When entering into a relationship, and then when subscribing for any new cash management product or service, we collect directly from you the data necessary for this operation.

These data are necessary:

- to enable us to fulfill our legal and regulatory obligations such as the obligation to know our client and our obligations regarding the fight against money laundering and the financing of terrorism,
- to know you, advise you and offer you the products and services that meet your needs,
- for the subscription of the product or service concerned,
- for its proper functioning.

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

You also provide us your contact details, including your email and cell phone number so that we can send you information as part of the service provision, to make notifications such as those related to the management of your contracts or for the realization of banking

operations, but also, upon acceptance, for the sending of commercial solicitations (mail, SMS, MMS).

Some personal data may be collected for regulatory or contractual purposes, or condition the conclusion of a contract. You are informed if necessary of the consequences of a refusal of communication.

For example:

- refuse to provide us with mandatory data for the opening and management of an account would not allow us to proceed with this opening,
- refuse to provide us with the information necessary to analyze your situation and your needs may prevent us from providing you with suitable advice.

The personal data coming from the use of banking products and services

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

The personal data coming from third parties or other services

The personal data can also derive from:

- third-party suppliers, subcontractors of BIC BRED's partners, if their data protection policies allow it,
- other products or services provided by third parties to which you have subscribed and for which you authorize the sharing with BIC BRED.

Public personal data

We may collect personal data publically available on you.

Public data are information or personal data produced or received by an administrative authority as part of its public service mission, published by an administrative authority or communicated to any person upon request.

We can use information or personal data which is public when permitted by laws and regulations and in compliance with the specific rules for communication and reuse specified by these texts.

Exclusion of special categories of personal data

The 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 in order to identify an individual uniquely, personal data concerning health or personal data concerning the sexual life or sexual orientation of a person.

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

Some of these data may nevertheless 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, to make a payment, or to sign electronically, using biometric recognition devices (voice recognition, facial recognition, fingerprints...). The use of this data helps to prevent fraud and the theft of your identity by a third party. These biometric recognition devices are alternative to other control mechanisms and are subject to specific security measures to ensure the security and confidentiality of personal data.

In any case, if we proceed with the processing of these special categories of personal data, and if it is not prohibited by any law or applicable regulations, your consent will be collected beforehand.

3. WHO ACCESSES YOUR DATA?

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

This same principle of secrecy and confidentiality applies to all stakeholders involved, be it our employees, our service providers, our partners and their own employees.

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

- BPCE SA acting as the central body of BPCE Group so that it can satisfy the various missions assigned to it by law, for the benefit of our institution and the Group, particularly with regard to prudential declarations to any competent regulatory authority, or data governance management purposes on behalf of BPCE Group institutions.
Data governance refers to the organization and procedures put in place to oversee the data collection and use practices within BPCE Group, and to optimize the efficiency of the use of this data in compliance with the legal and ethical framework.
- Any entity of BPCE Group in order to be able to present to you products or services managed by these entities.
- To entities belonging to our group (BPCE, Banques Populaires / Caisses d'Epargne, Natixis Assurance, Natixis Financement, Natixis Lease...) for the study or development of all types of contracts or transactions which may concern you.
- Any entity of BPCE Group with who you enter or have entered into a contractual relationship for the purpose of updating the data related to your marital status, family status, assets and

finances, the operation of your account and the assigned score for the application of banking regulations, collected by these entities, including information relating to your fiscal status. This data can also be used for the study of your file, the use of the products and / or services subscribed or their recovery.

- To entities, which are subcontractors of BPCE Group, in case of pooling of technical means, including IT Services on behalf of our institution. To this end, the personal data may be pseudonymised for purposes of research and statistical model creation. Pseudonymisation means that the concerned data can no longer be linked to you without the use of additional information, kept separately and subject to technical and organizational measures to ensure that the original data can no longer be attributed to an identified or identifiable person.

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

- With third parties (service providers, subcontractors, etc.) with the goal to allocate to them the operational functions;
- with the partners of BIC BRED, allowing you to enjoy the benefits of a partnership to which you previously decided to adhere, and in the exclusive setting of the partnership agreements;
- with subcontractors and service providers for the sole purpose of the services to be performed on our behalf and in particular the provision of banking and financial services or products or the carrying out of surveys or statistics.

We share your personal data in the following cases :

- when expected in this notice,
- when necessary to provide to you the products, and services purchased,
- when you consent to this sharing.

We must also share your data when the professional secrecy is lifted by the law and in particular with regard to the tax administration and the customs, the Banque de France, the social security organizations, the parliamentary commissions of investigation. Secrecy is also lifted with regard to the information required for the application of the agreements concluded by French organizing an automatic exchange of information for tax purposes. Secrecy can only be opposed to the judicial authority acting in criminal proceedings, as well as in civil proceedings where a specific text expressly predict this.

4. WHY ARE WE PROCESSING 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 principles :

Execute the contract for products and services that you have subscribed to or wish to subscribe

We primarily process your personal data in order to provide you with the products and services you underwrote, or which you want to underwrite.

The processing is implemented because it is necessary for the execution of the contract, or the execution of pre-contractual measures taken at your request as a customer, within the framework of an already established relationship, or as a prospect if no business relationship has yet been established (pre-contractual measures such as the issuance of an advice, a proposal, a simulation).

The implemented processing for the management of our relationship concerns in particular the maintenance of your payment accounts and the execution of operations, the management of your products and services as well as the management of their functioning and the security of the payment transactions.

Without these processes, we would not be able to conclude or execute the contract.

Prior to the authorization of a payment transaction, we can implement an automated decision-making based in particular on the analysis of the payment information, the context of the transaction, the balance of the account on which the instrument operates and which takes into account payment limits. Automated decision making may result in the authorization or refusal of the payment transaction.

Meet our legal and regulatory obligations

Our activity operates in a highly regulated regulatory environment for the execution of payment transactions.

To meet these legal obligations, we are implementing the processing of personal data.

As a result, we may be required to request specific information regarding certain transactions if we are required by law or regulation.

Fight against money laundering and terrorist financing

We are obliged to proceed to the identification of our customers and, where applicable, the actual beneficiaries of operations and we have a duty of constant vigilance of our customers for the duration of the business relationship (amount and nature of operations, provenance and destination of funds, follow up of the

professional, economic and financial situation of our client, etc.). The information you communicated us as such must be regularly updated.

As such, we are required to apply special vigilance measures in respect of Politically Exposed Persons as defined by Regulation.

We are also required to report to the appropriate authorities some transactions and in particular:

- amounts in our books and transactions involving money that could come from an offense punishable by deprivation of liberty or that may be involved in the financing of terrorism,
- transactions for which the identity of the payer or the beneficial owner of the transaction remains doubtful despite the due diligence carried out under the obligation of verification of identity which is mandatory for the payment institution.

Information required for maintaining regulatory files

We communicate the personal data following from certain regulatory obligations such as **responses to requests for exercising rights** under the regulations on the protection of personal data. The exercise of your rights, referred to in Article 11 of this document, requires the processing of your personal data for the purpose of identification, management of your requests and retention of evidence.

Answering to our legitimate interests

We can invoke a "legitimate interest" to process your data, especially when we find ourselves in situations that may pose risks to our business, such as preventing fraud in particular on payment instruments and manage possible legal actions , fight against financial crime both with regard to the financial sector and with regard to our customers and employees, to prevent and manage incivilities with regard to of our employees, to ensure the security of our networks and information, to monitor access to our premises in particular by a video surveillance device .

Our legitimate interest may also be linked to the management of our business as a company (financial accounting, invoicing, stock management, reporting, statistical studies and satisfaction surveys), the management of our customer relations (improving customer knowledge, improve our products and services), prospecting, profiling and marketing segmentation including appropriate combination of data for analysis or anonymization, or for our audit work, inspection and communication.

These processes are implemented taking into account your interests and fundamental rights. As such, they are accompanied by measures and safeguards to ensure a balance between the protection of your interests and rights and the pursuit of our legitimate interests.

Implementation of some processes with your consent

We can run some processes when you have consented to one or more specific purposes.

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

Thus, when we wish to proceed with the commercial prospecting by e-mail, we collect your prior consent to send commercial offers.

5. HOW LONG ARE YOUR DATA KEPT?

Once the final duration of keeping the data is reached taking into account any legal or regulatory obligations imposed to keep some data, we delete or anonymize your data.

The duration of keeping data is variable and depends on the nature of the data and the purposes pursued.

Personal data collected in order to manage a contract

The data are kept for the period of time necessary for the performance of the contract and until the expiry of the applicable legal deadlines.

Different delays can apply :

- in accordance with the general limitation period the accounting documents and supporting documents must be kept for a period of **10 years**. The personal data necessary for the performance of this obligation will therefore be retained during this period. The period of 10 years generally runs from the date of the transaction. For example, for an operation registered in your payment account, the retention period of the data related to this transaction will be 10 years from the date of the transaction,
- the same applies to the data relating to your account , kept for a period of 10 years from the closing of your account or the termination of our relationship ,
- the delays for specific legislation such as the fight against money laundering and the financing of terrorism are 5 years ,
- the delay necessary for the intended purpose, for example, in the fight against fraud this is 5 years.

These periods may be longer in specific situations when legally required or in case of litigation. In this case, the

data are kept until the end of the legal proceedings and archived according to the applicable legal prescription periods.

When a personal data is collected for several purposes, it is retained until exhaustion of the longest retention or archiving period.

After the termination of the relationship, we may also keep your data and exploit some of this information (your name, surname, address, date and place of birth, characteristics of the product previously subscribed) for the purpose of commercial prospecting for a maximum duration of 5 years (from the last incoming contact) . You may at any time object to the processing carried out for purposes of commercial prospecting under the conditions provided for in article 11 hereof.

Personal data collected for a pre-contractual context, without an actual conclusion of a contract

When you have contacted us to request a product or service or a simulation and that your application has not been followed by a subscription, we keep your data for a period limited to the purpose initially pursued (for example, to be able to reissue a simulation, or to keep track of the advice which we gave you).

Personal data relating to a non-customer prospect

The personal data relating to a non-customer prospect is kept, for commercial prospecting purposes, for a maximum duration of 3 years from the last contact from the prospect.

This data is also kept for 5 years for the purpose of fighting money laundering and the financing of terrorism and the fight against fraud.

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

Respect for privacy and bank secrecy, security and confidentiality of data and especially personal data entrusted by our customers is our priority.

We take, in view of the nature of the personal data and the risks presented by the processing, technical and organizational measures to safeguard the security of your data and, in particular, prevent it from being distorted, damaged, or that unauthorized third parties have access to it or prevent it from being misused.

Thus, we are committed to take the physical, technical and organizational security measures necessary to :

- preserve the security of personal customer data against unauthorized access, alteration, distortion, disclosure or destruction of personal data held by us,
- protect our activities.

We organize regular internal audits to ensure the security of personal data and to safeguard ourselves against unauthorized access to our systems.

Nevertheless, the security and confidentiality of personal data is based on best practices of each, so you are invited to remain vigilant.

In order to protect the confidentiality of your personal data, we invite you, especially in rules related to the Internet use, to take all necessary measures including deleting, at the end of your consultation, traces of browsing and preventing access to unauthorized third parties should you upload this data to management software.

In accordance with our commitments, we choose our subcontractors and service providers with care and impose them :

- a level of personal data protection equivalent to ours,
- access and use of data personal information or information strictly necessary for the services which they must provide,
- strict compliance with the law and applicable regulations privacy, bank secrecy and personal data,
- the implementation of all appropriate measures to ensure data protection personal data that they may have to deal with
- the definition of technical and organizational measures necessary to ensure data security.

We are committed to conclude with our subcontractors, in accordance with legal and regulatory obligations, contracts precisely defining the terms and conditions of processing of personal data.

7. WHERE IS YOUR DATA STORED?

Personal data and information relating to our customers is stored in our information systems or that of our subcontractors or suppliers.

We are committed to selecting subcontractors and service providers that meet the quality and safety criteria, and that offer sufficient guarantees, particularly in terms of specialized knowledge, reliability and resources, for the implementation of technical and organizational measures including the safety of the processing.

As such, we impose on our subcontractors and our service providers' confidentiality rules at least equivalent to ours.

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

Is your data communicated or accessible from a country in the European Union ?

Your personal data transmitted in accordance with the intended purpose may, during various operations, be transferred to a country of the European Union.

In case of transfer of funds, some personal data must be transmitted to the bank of the beneficiary of the transfer in a country of the European Union.

These personal data can be communicated, at their request, to official bodies and administrative or judicial authorities empowered, or to third parties.

In any case, we take the necessary and appropriate steps to ensure the secrecy and security of personal data.

8. OUR PROSPECTING ACTIONS

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

You can object at any time with no charge to actions initiated for marketing purposes, as further specified in Article 11 hereof.

Phone prospection

We may need to prospect by telephone.

You are informed that you can sign up on a list of opposition to the telephone canvassing. However, despite this registration, we can contact you by telephone if there are existing contractual relationships unless you oppose it or if you object to it during the call.

9. IMPLEMENTATION OF SPECIAL PROCESSES BASED ON SPECIFIC TECHNOLOGY

Cookies and other tracers

With "Cookies or other tracers" we mean the tracers deposited and read, for example during the consultation of a website, the reading of an email, the installation or use of a software or a mobile application, regardless of the type of device used.

You are informed that during your visits to one of our websites, cookies and tracers may be uploaded on your device. You can consult, on the concerned website, the cookie policy. When necessary we collect your consent prior to the installation on your terminal equipment of such tracers but also when we access data stored on your equipment.

The lifetime of these tracers is 13 months maximum.

Phone recording

Phone conversations between you and our services may be recorded for the purpose of training, evaluation or improvement of the quality of products and services or evidence of past remote operation.

Prior to a registration, we inform you.

The recording media or their reproduction will be kept for periods proportionate to the purpose of the recording in question.

10. YOUR RIGHTS

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

- **access** to all your personal data,
- **rectify, update and delete** your data personal, it is specified that the erasure can only occur when :
 - o personal data are no longer necessary for the purposes for which they were collected or otherwise processed,
 - o you have withdrawn your consent on which the process was based,
 - o you opposed to the processing of data and there is no compelling legitimate grounds to continue,
 - o personal data have been subject to unlawful processing
 - o personal data must be erased in order to comply with a legal obligation provided for by the law of the Union

or by French law to which BIC BRED is subject.

- **oppose** to the processing of personal data for reasons specific to you,
- **oppose** to the processing of personal data for purposes of **commercial prospecting**,
- **receive** personal data about you that you have provided to us, for automated processing based on your consent or the performance of a contract , and to request the portability of such data,
- **ask for a limited processing** of personal data that we operate about you when :
 - o you contest the accuracy of the personal data and for a time allowing the controller to verify the accuracy of personal data,
 - o you oppose to the erasure of your data while the processing is illegal ,
 - o we no longer need the data but these are still required by you for the recognition, exercise or defense of rights justice,
 - o you are opposed to the processing of your data, while checking on the question whether the legitimate reasons pursued by BIC BRED prevail over yours.
- where the processing is based on your consent, **withdraw that consent** at any time,
- **file a complaint** with a supervisory authority.

You must provide proof of your identity by clearly indicating your name and surname, the address to which you wish the answer to be sent to you, sign your application and attach a photocopy of an identity document bearing your signature.

The exercise of your rights of access, of rectification, opposition, erasure, your right to limitation of processing or data portability personal is done without charge.

Under the exercise of the right of access, we will provide you with a copy of personal data undergoing processing. In the case of requests which are manifestly unfounded or unreasonable, in particular because of their repetitive nature, we may demand the payment of reasonable charges, taking into account the administrative costs incurred in providing such information, making communications or making the requested measures , or refusing to answer to your request.

This information notice is subject to change. The latest version in force can be consulted at the following address: www.bred.fr

In France, the supervisory authority is:

CNIL - 3 place de Fontenoy - TSA 80715
75334 PARIS CEDEX 07
www.cnil.fr

11. HOW TO EXERCISE YOUR RIGHTS

If you wish to learn more about the provisions of this information sheet, please write to the following address:

BRED Banque Populaire
Délégué à la Protection des Données
4, route de la Pyramide
75132 PARIS CEDEX 12

By email: delegue-protection-donnees@bred.fr

You can also exercise your rights by making your request to your Sales Representative. He will accompany you in the steps described below.