DATA PROTECTION NOTICE

Last updated 22/7/2025

Preliminary section: Main amendments

As a trusted companion, the protection of your personal data is important to the BNP Paribas Group.
We have revised our Data Protection Notice to improve transparency and provide further information on our processing of your personal data, including but not limited to personal data processing in the context of:

- business to business and/or direct marketing; and
- anti-money laundering, countering the financing of terrorism and international sanctions (freezing of assets).

Introduction

We take the protection of your personal data very seriously.

BNP Paribas (including its subsidiaries) in relation to its Corporate and Institutional Banking (CIB) business ("we", "our"), as a controller, is responsible for collecting and processing your personal data in relation to our banking activities which include capital markets services, securities services, financing, treasury and advisory services.

The business of the BNP Paribas Group is to help all of their clients: individuals; entrepreneurs; small and medium-sized enterprises; large companies; multi-national groups and institutional investors, in all of their activities from their day-to-day banking requirements to their commercial objectives and projects, by providing appropriate financing, investment, multi-asset servicing, savings and insurance solutions.

As a member of an integrated banking and insurance group, in collaboration with the various entities of the Group, we provide our clients with a complete range of banking, insurance and leasing products and services.

Whether under the European Union's General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016) and/or other applicable data protection legislation, the purpose of this Data Protection Notice is to inform you of: the personal data we collect about you; the reasons why we use and share such data; how long we keep the data; what your rights are (as to the control and management of your data) and how you can exercise your personal data rights.

Further information may be provided where necessary at the time of collection of your personal data.

1. ARE YOU SUBJECT TO THIS NOTICE?

This Data Protection Notice applies to you ("you") if you are:

- an employee, consultant, contractor, legal representative, shareholder, investor, or beneficial owner of:
  - a client;
  - a prospective client;
  - a client or counterparty of our clients(s); or
  - a counterparty;
- a beneficiary of financial transactions (payment or shares) or contracts, policies, or trust;
- an ultimate beneficial owner in the context of our services;
- a company shareholder;
- a social network user.

In certain circumstances, we collect information about you even if we do not have a direct relationship with you. This indirect collection of information about you may happen, for instance, in the course of our relationship with our clients or counterparties.

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 Data Protection Notice, as it provides them useful information about their rights. 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 EXERCISE YOUR RIGHTS IN THE CONTEXT OF OUR PERSONAL DATA PROCESSING?

You have rights under, and in accordance with, applicable data protection law which allows you to exercise real control over your personal data and how we process it.

Should you wish to exercise the rights summarised below please refer to section 9 (How to contact us) and section 11 (Country-specific provisions) as appropriate.

2.1. You can request access to your personal data

We will provide you with a copy of your personal data promptly upon request, together with information relating to its processing.

Your right of access to your personal data may, in some cases, be limited by applicable law and/or regulation. For example, regulations relating to anti-money laundering and countering the financing of terrorism 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 your data protection authority (details of which are listed in Appendix B), which may request the data from us.

2.2. You can ask for the correction of your personal data

Where you consider that your personal data is inaccurate or incomplete, you can request that we modify or complete such personal data. In some cases, you may be required to provide supporting documentation.

2.3. You can request the deletion of your personal data

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

2.4. You can 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 your 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 defence of legal claims.

2.5. You can object to the processing of your personal data for direct marketing purposes

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

2.6. You can suspend the use of your personal data

If you query the accuracy of the personal data we use, we will review and/or verify the accuracy of such personal data. If you object to the processing of your personal data, we will review the basis of the processing. You may request that we suspend the processing of your personal data while we review your query or objection.

2.7. You have rights against an automated decision

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or otherwise significantly affects you. However, we may automate such a decision if it is necessary for the entering into or performance of a contract between us, authorised by law or regulation; or if you have given your explicit consent.

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

2.8. You can 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. You can request the portability of part of your personal data

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

2.10. How to file a complaint with your supervisory authority

In addition to the rights mentioned above, you may lodge a complaint with the relevant data protection authority, which is usually the one in your place of residence. A list of data protection authorities is set out at Appendix B.

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

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

3.1. Your personal data is processed to comply with our various legal and/or regulatory obligations

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

3.1.1. We use your personal data to:

- monitor operations and transactions to manage, prevent and detect fraud ;
- monitor and report risks (financial, credit, legal, compliance or reputational risks, operational risks etc.) that we/and or **the BNP Paribas Group could incur;**
- record, retain and report transactions and communication in compliance notably with the Markets in Financial Instruments Directive II. This includes maintaining records of transactions and communications in any form, including voice and electronic communications, for instance in the context of the provision of services relating to orders, in particular their receipt, transmission, execution and recording;
- detect, prevent, manage and report suspicious orders, transactions and behaviors (e.g. market abuse), notably in the context of the Market Abuse Regulation and ensure the transparency of financial transactions in markets by monitoring transactions and voice and electronic communications when necessary;
- communicate, in compliance with the Shareholders Rights Directive your personal data to issuers, including your shareholder identification, proxy voting and register information;
- assist the fight against tax fraud and fulfil tax control and notification obligations, including in the context of US Foreign Account Tax Compliance Act and Automatic Exchange of Information obligations;
- fulfil our obligations to declare and register transactions with the competent authorities (tax, judicial, criminal, etc);
- record transactions for accounting purposes;
- prevent, detect and report risks related to Corporate Social Responsibility and sustainable development;
- detect and prevent bribery and corruption;
- exchange and report different operations, transactions or orders or reply to an official request from duly authorized local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, law enforcement, state agencies or public bodies.

3.1.2. We also process your personal data 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 which may require the processing of your personal data primarily through our Know Your Customer (KYC) process (to identify you, verify your identity and screen your details against sanctions lists, prior to and in the course of our services).

In the context of this processing we, [as a branch or subsidiary of BNP Paribas SA], 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 Appendix A.

3.2. Your personal data is processed to perform a contract with you in the context of our services to our clients and/or counterparties

Your personal data is processed when it is necessary to enter into or perform a contract to provide our corporate clients with the products and services subscribed to under the applicable contract, including access to our digital services.

3.3. Your personal data is processed to fulfil our legitimate interest or that of a third party

Where we base a processing activity on legitimate interest, we balance that interest against your interests and 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 activity, please contact us using the contact details provided in section 9 (How to contact us) below.

3.3.1. In the course of our business as a bank, we process your personal data to:

- Manage your access to and use of our web communication channels and applications in the context of our contractual and pre-contractual relationships with our clients; counterparts; and/or service providers.
- communicate with you in the context of services provided to our clients and counterparties;
- manage our activities and our presence on social networks (see more details in section 5.1).
- manage the risks to which we are exposed:
    - we keep evidence of, and sometimes record operations, transactions and communications when you interact with our employees (eg. in our chat rooms, via emails, or during video conferences);
    - we monitor transactions to manage, prevent and detect fraud including, where required by law, the establishment of a fraud list (which will include a list of fraudsters);
    - we manage legal claims and defend our position in the event of litigation.
- enhance cyber security and data leakage prevention measures, manage our platforms and websites, and ensure business continuity.
- use video surveillance to monitor access to property and prevent personal injury and damage to people and property.
- record, retain, monitor and report transactions and voice and electronic communications in order to comply with our code of conduct, internal policies and procedures, applicable third country laws and regulations to which we are subject as a financial institution including those on recording and recordkeeping of voice and electronic communications, market abuse, market integrity surveillance of voice and electronic communications, or to establish proof of contract formation.
- enhance the automation and efficiency of our operational processes and client services (e.g., automatic filing of complaints, tracking of your requests and improvement of your satisfaction based on personal data collected during our interactions with you such as phone recordings, e-mails or chats).
- comply with the provisions applicable to trust service providers issuing electronic signature certificates.
- carry out financial operations such as debt portfolio sales, securitizations, financing or refinancing of the Group.
- perform our asset management services any time you are an indirect beneficiary of these services, including the following purposes:
    - the creation and maintenance of your shareholder or investor register;
    - the receipt, capture and processing of your shareholder's voting instructions;
    - tax services performed on your behalf (*ie* relief at source, tax reclaim);
    - the safekeeping of your physical securities ;
    - the management of your access and use of our web communication channels and applications;
- conduct statistical studies and develop predictive and descriptive models for:
    - commercial purposes: to identify the products and services that could best meet your needs, to create new offers based on trends arising from our web communication channels and application use, to develop our commercial policy taking into account our clients' preferences
    - safety purposes: to prevent potential incidents and enhance safety management;

- compliance and risk management purposes (eg., anti-money laundering and countering the financing of terrorism);
- anti-fraud purposes.

3.3.2. We use your personal data to send you commercial offers by electronic means, post and phone

As part of the BNP Paribas Group, we want to be able to offer you access to the full range of products and services that best meet your needs.

If you are identified as a contact or representative of a client; or counterparty, and unless you object, we may send you offers by any means for our products and services and those of the Group.

We will use reasonable endeavours to ensure that these offers relate to products or services that are relevant to our clients or prospective clients' activities.

3.4. Your personal data is processed if you have given your consent

For some personal data processing activities, we will give you specific information and ask for your consent. Of course, you can withhold your consent or, if given, withdraw your consent at any time.

In particular, we ask for your consent to:

- Manage newsletter subscriptions;
- Manage events;
- Use your navigation data to enhance our knowledge of your profile in accordance with our Cookies Policy.

You may be asked for further consent to process your personal data where necessary.

4. WHAT TYPES OF PERSONAL DATA DO WE COLLECT?

We collect and use your personal data, meaning any information that identifies or, together with other information, can be used 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, identity (e.g. copy passport, driving licence), nationality, place and date of birth, gender, photograph);
- **contact information** private or professional (e.g. postal and e-mail address, phone number etc.);
- **family situation** (e.g. marital status, number and age of children etc.);
- **lifestyle** (hobbies and interests);
- **economic, financial and tax information** (e.g. tax ID, tax status, fiscal address, income and others revenues, value of your assets);
- **education and employment information** (e.g. level of education, employment, employer's name, remuneration);
- **banking and financial information** (e.g. bank account details, products and services owned and used, credit card number, money transfers, assets, declared investor profile, credit history, any defaults in making payments);
- **transaction data** (including full beneficiary names, address and transaction details including communications on bank transfers of the underlying transactions);
- **data relating to your habits and preferences** (in relation to the use of our products and services);
- **data from your interactions with us or about us**: meeting and contact reports, data shared on our websites, our apps and social media pages;
- **data related to the recording and/or surveillance of voice and electronic communications** (e.g. voice calls, videoconferences, instant messages, emails, SMS…)
- **connection and tracking data** such as cookies, connection to online services, IP address, meetings, calls, chats, emails, interviews, phone conversations;
- **video protection** (including CCTV);
- **information about your device** (including MAC address, technical specifications and uniquely identifying data); and
- **login credentials used to connect to BNP Paribas' website and apps**.

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.

Please note that you are not required to provide any of the personal data that we request. However, your failure to do so may result in us being unable to provide our services.

5. WHO DO WE COLLECT PERSONAL DATA FROM?

We may collect personal data directly from you as staff of our clients, counterparties and their service providers in the context of our activities and services.

We sometimes collect data from public sources:

- publications/databases made available by official authorities or third parties (e.g., the Official Journal of the French Republic, the Trade and Companies Register, databases managed by the supervisory authorities of the financial sector);
- 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 other Group entities;
- from our business partners or our clients' business partners;
- from service providers (e.g. payment initiation providers, service providers of account information such as account aggregators);
- from credit reference agencies and fraud prevention agencies.

5.1. Personal data collection via social network

In today context, use of social network is essential to companies.

In order to fulfill efficiently our mission, it is essential for us to be present on social networks, and this presence is susceptible to involve the processing of some of your personal data.

Therefore, in our legitimate interest of needs in marketing, communication, advertising, and publications, as well as for crisis management and interaction with social media users, we are susceptible to collect the following personal data:

- The exchange that you had with us on our pages and publications on social networks, including your early claims and complaints.
- Data coming from pages and publications on social networks that contain information that you publicly made available.

More specifically, these personal data will be treated for the following purposes:

- Crisis management (social listening) and customer relationship management, this includes:
  - Crisis prevention: Monitoring and analysis of social networks and the web by using keywords to assess BNP Paribas reputation and be aware of what is said about a trending/crisis topic in order to communicate accordingly.
  - Crisis management handling: Analyze the problematics raised by some publications and act accordingly; answer to publications, posts or comments of social network users; identify and tackle fake accounts and fake publications; or investigate in case of strong allegations and claims.
- Marketing and communication/ advertisement and publications which includes:
  - Data extraction to identify trending topics by collecting data publicly available on social networks;
  - Publication of articles;
  - Suggestion of publications according to your interests;
  - Customer and social network users' segmentation according to their influence;
  - Advertisement optimization/targeted marketing by segmenting the recipients of the marketing/advertisement.

In order to achieve this, we use external service providers.

6. WHO DO WE SHARE YOUR PERSONAL DATA WITH AND WHY?

a. With BNP Paribas Group's 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 Group entities, where necessary, to:

- comply with our various legal and regulatory obligations described above;
- fulfil our contractual obligations or legitimate interests described above; and
- conduct statistical studies and develop predictive and descriptive models for business, security, compliance, risk management and anti-fraud purposes;

Sharing with Group companies may extend to intragroup processors which perform services on our behalf (such as our hubs in India, Poland and Portugal).

b. With recipients outside the BNP Paribas Group

In order to fulfil some of the purposes described in this Data Protection Notice, we may, where necessary, share your personal data with data processors which perform services on our behalf (e.g., IT service providers, logistics, printing services, telecommunication, debt collection, advisory and distribution and marketing).

We may also, where we consider it necessary, share your personal data with other data controllers, as follows:

- banking and commercial partners, independent agents, intermediaries or brokers, financial institutions, counterparties, trade repositories with which we have a relationship if such transmission is required to allow us to provide you with the services and products or execute our contractual or legal obligations or process transactions (e.g., banks, correspondent banks, depositaries, custodians, issuers of securities, paying agents, exchange platforms, insurance companies, payment system operators, issuers or payment card intermediaries, mutual guarantee companies or financial guarantee institutions);
- regulators and/or independent agencies, local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, public authorities or institutions (e.g., the *Banque de France* and *other Central Banks*), to which we, or any member of the BNP Paribas Group, are required to disclose pursuant to:
    - their request;
    - our defence, action or proceeding;
    - complying with a regulation or a recommendation issued from a competent authority addressed to us or any member of the BNP Paribas Group;
- service providers or third-party payment providers (information on your bank accounts), for the purposes of providing a payment initiation or account information service at your request;
- certain regulated professions such as lawyers, notaries, or auditors particularly 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 Group.

7. INTERNATIONAL TRANSFERS OF PERSONAL DATA

In certain circumstances (e.g. to provide international services or to ensure operational efficiency), we may transfer your data to another country. This includes transfers of personal data to our branches and subsidiaries in APAC and the Americas.

In case of international transfers originating from:

- the European Economic Area ("EEA") to a non-EEA country, the transfer of your personal data may take place where the European Commission has recognised a non-EEA country as providing an adequate level of data protection. In such cases your personal data may be transferred on this basis;
- the United Kingdom ("UK") to a third country, the transfer of your personal data may take place where the UK Government has recognised the third country, as providing an adequate level of data protection. In such cases your personal data may be transferred on this basis;

- other countries where international transfer restrictions exist, we will implement appropriate safeguards to ensure the protection of your personal data.

For other transfers, we will implement an appropriate safeguard to ensure the protection of your personal data, being:

- Standard contractual clauses approved by the European Commission or the UK Government (as applicable); or
- Binding corporate rules.

In the absence of an adequacy decision or an appropriate safeguard we may rely on a derogation applicable to the specific situation (e.g., if the transfer is necessary for the exercise or defence of legal claims).

You can obtain more details about the basis of our international transfers by sending written request to gdpr.desk.cib@bnpparibas.com.

8. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We will retain your personal data for the longer of:

- the period required by applicable law;
- such other period necessary for us to meet our operational obligations, such as: proper account maintenance, facilitating client relationship management, and/or responding to legal claims or regulatory requests.

Most personal data collected in relation to a specified client is kept for the duration of the contractual relationship plus a specified number of years after the end of the contractual relationship or as otherwise required by applicable law.

If you would like further information on the period for which your personal data will be stored or the criteria used to determine that period please contact us at the address given under section 9 (How to contact us) below.

9. HOW TO CONTACT US?

If you wish to exercise the rights summarised in Section 2 (How you can exercise your rights in the context of our personal data processing), if you have any questions relating to our use of your personal data under this Data Protection Notice, or if you would like a copy of this Data Protection Notice in your native language, please contact gdpr.desk.cib@bnpparibas.com or the email specified for your country under Section 11. In some cases, you may be required to provide evidence of your identity.

10. HOW TO FOLLOW THE EVOLUTION OF THIS DATA PROTECTION NOTICE?

We regularly review this Data Protection Notice and update it as required.

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

11. COUNTRY-SPECIFIC PROVISIONS

Czech Republic

Data Subject Rights

We, BNP Paribas entities registered in Czech Republic, including BNP Paribas S.A., registration number 662042449 RCS Paris, with its registered office at 5009 Paris, 16 Boulevard des Italiens, France, acting in the Czech Republic through its branch office **BNP Paribas S.A., pobočka Česká republika**, will not require you to include a scan/copy of your identity card for identification purposes, if you wish to exercise the rights listed in section 2 above. Instead, for identification purposes, you can,

• Visit BNP Paribas entities registered in Czech Republic in person.
• Send an original letter with your hand signature which has been verified by a notary public.
• Send as an email with your qualified electronic signature.

Complaints

In accordance with applicable regulation, you are also entitled to lodge a complaint with the competent supervisory authority. The contact details of the supervisory authority in the Czech Republic is:

ADDRESS: Czech Office for Personal Data Protection (Úřad pro ochranu osobních údajů), Pplk. Sochora 27, 170 00 Prague 7, Czech Republic

TELEPHONE NUMBER: +420 234 665 111

EMAIL: posta@uoou.cz

DATA BOX: qkbaa2n

Changes to this Data Protection Notice

We may need to update this Data Protection Notice from time to time. We will inform you of any material changes through our website: https://www.bnpparibas.cz/en/