BANCO BPM

PRIVACY NOTICE (CLIENTS)

Last Updated: June 2026

Dear Client, this privacy notice provides the information necessary to understand how Banco BPM S.p.A. (hereinafter also the "Bank") processes your personal data. You may consult this notice at any time by accessing the website gruppo.bancobpm.it/en, in the Privacy section. The text has been organized into sections, so as to enable you to easily identify the topics of interest to you. We provide you with this notice before proceeding with the processing of your personal data, as required by Articles 13 and 14 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "Regulation").

1. Data Controller and Data Protection Officer



The Data Controller determines the purposes and means of the processing of your personal data, adopting appropriate measures to ensure their protection. Banco BPM S.p.A., with registered office at Piazza F. Meda, 4, 20121 Milan, acts as Data Controller. The Data Protection Officer (the "DPO") is appointed by the Bank to ensure the proper processing of personal data and may be contacted, for matters relating to data processing and to exercise the rights provided for by the Regulation, at the following contact details: email: protezionedati@bancobpm.it; certified email (PEC): protezionedati@pec.bancobpmspa.it; postal address: "For the attention of the DPO – Data Protection Officer", Banco BPM, Piazza F. Meda, 4, 20121 Milan.

For the processing of personal data, the Bank relies on third parties (data processors, joint controllers and other data controllers), whose list is available upon request via the contact details above.

2. Recipients of this Privacy Notice

This privacy notice is addressed to data subjects who:

- have entered into a contractual relationship with the Bank or are about to enter into such relationship (for example, clients who have opened or are in the process of opening a current account);
- carry out an occasional transaction (for example, a data subject who does not hold a current account and visits a Bank branch to make a payment);
- are connected to the client of the Bank (for example, legal representatives, directors, shareholders, beneficial owner, attorneys, delegates or authorized signatories) whose data are collected or communicated to the Bank in the context of the relationship with the client. If you provide third-party data, ensure they receive this notice beforehand.

3. Purposes of the processing and legal basis

Personal data may be processed only for purposes based on a legal basis provided by the Regulation. The Bank processes your data to:



- properly manage the relationship and the activities connected thereto, both in the phase in which the relationship has been established ("contractual") and in the preceding phase ("pre-contractual"). Activities connected to the relationship include, for example, credit and financial services, the management of movable and immovable assets, debt collection, the management of insurance activities and related services, as well as the assessment of the quality of the services provided. Processing of your data for these purposes does not require your consent; if you refuse to provide the data, it will not be possible to establish or perform the relationship. The legal basis is Article 6(1)(b) of the Regulation;
- comply with obligations established by law and with provisions issued by Authorities or judicial bodies. Such obligations include, by way of example, provisions of civil, criminal, tax, EU and supervisory law, as well as rules, codes and procedures approved by Authorities and other competent institutions (for example: tax assessments, anti-money laundering, anti-corruption), as well as rules on the monitoring and uniform classification of operational and credit risks, including at banking group level. Processing of personal data for these purposes is necessary to comply with a legal obligation to which the Bank is subject and does not require your consent; if you refuse to provide the data, it will not be possible to establish or perform the relationship. The legal basis is Article 6(1)(c) of the Regulation.

3.1 When your consent is required

If you provide your consent (which must be freely given, specific, informed and unambiguous), the Bank may process your data, mainly by automated means (for example, email, telephone, internet, apps and other communication systems) as well as by paper-based means, in order to carry out:

- market research and analysis activities;
- activities related to the promotion and sale of products and services (of Banco BPM Group companies and third-party companies), also identified through the processing of information that makes it possible to analyse preferences, habits and consumption choices (so-called customer profiling). The Bank may acquire this information internally (through the analysis of current account transactions, credit cards, prepaid cards and the overall financial situation, including navigation within the personal area of the Bank's website and app), or from external sources (so-called enrichment of the Bank's database). The processing of this information makes it possible to classify customers into homogeneous categories based on behaviours or specific characteristics, in order to offer products and services consistent with their needs.

Processing of the data indicated above is not mandatory for the performance of the contract; for this reason, your consent is required, in the absence of which you will not be able to receive marketing communications tailored to you. The legal basis is Article 6(1)(a) of the Regulation.

3.2 When processing is based on legitimate interest

The Bank may process your data in order to pursue a legitimate interest, either its own or that of third parties, provided that such interest is balanced against the reasonable expectations of the client and that your interests and fundamental rights and freedoms are not overridden. If you object, the Bank will cease the processing, unless there are compelling legitimate grounds for continuing, which override your interests, rights and fundamental freedoms. You may exercise your right to object by following the procedures set out in the section "Data subjects' rights". The legal basis is Article 6(1)(f) of the Regulation. The Bank's legitimate interests include processing data for the following purposes:

- to carry out activities aimed at implementing corporate or financial transactions, including those between companies of the Banco BPM Group, such as, for example, securitisations, transfers of receivables and the issuance of securities, transfers of companies and business units, mergers, demergers, including extraordinary transactions within restructuring or insolvency proceedings (e.g. bankruptcy or liquidation);
- to implement commercial collaborations, including within the Group, in order to improve the integrated use of technical solutions supporting business processes;
- to prevent risks of fraud in payments and other risks required by the regulations to which the Bank is subject, giving rise to legal obligations (for example anti-money laundering). For this purpose, personal data may be compared with those contained in external databases;
- to ensure IT security, the proper management of IT systems and business continuity (so-called "business continuity");
- to develop and update models aimed at better understanding clients' needs, based on the analysis of quantitative and qualitative data, in order to offer increasingly suitable products and services and maintain a competitive standard in the market;
- to establish, exercise or defend legal claims in any context.

4. Categories of data processed

For the purposes indicated in this privacy notice, the Bank processes personal data that fall, by way of example, within the following categories:



- identification, personal and contact data, for example, name, surname, date and place of birth, nationality, tax code, VAT number, identification document and the image contained therein, residential and domicile address, email address/certified email (PEC), landline/mobile phone number, IP address, as well as data relating to call recordings and to the use of our products and services;
- financial data, for example, IBAN, credit card number, debit card number, prepaid card number, current account/securities account balances, transaction data, data relating to financial situation and credit information relating to credit applications and credit relationships.

In order to provide the services and carry out the requested transactions, the Bank may also process special categories of personal data, such as, by way of example, information relating to health, political opinions, religious or philosophical beliefs, or trade union membership. In such cases, your consent is required, except where the Regulation allows processing without it. Where permitted by applicable law, data relating to criminal convictions and offences or to security measures may also be processed.

5. Source and methods of processing of personal data



Personal data processed by the Bank may be collected directly from the client, from third parties or from publicly available sources (for example, Company Registers, Chambers of Commerce or Credit Information Systems). When the execution of a transaction or the opening of a relationship is requested, data relating to third parties, such as guarantors or beneficial owners, may also be collected.

The Bank processes all personal data that you provide or that may be communicated to us by third parties, in compliance with the applicable data protection legislation and in accordance with the principles of fairness, lawfulness and transparency, and for the purposes indicated. Data are collected to the extent necessary and appropriate for the processing, using only authorised and duly trained personnel, and in order to ensure the confidentiality of the information provided. The Bank processes personal data by means of both paper-based and IT tools and may develop and use artificial intelligence systems to improve and make the processes of the Banco BPM Group more efficient. Such systems, based on machine learning techniques, may generate predictions or recommendations to support the Bank's activities, for example in creditworthiness assessments or fraud prevention activities. For their design and training, only personal data strictly necessary for such purposes are used and, where possible, anonymised or synthetic data. All artificial intelligence systems are subject, from the design phase, to specific safeguards aimed at ensuring the adoption of the necessary measures to protect the client's fundamental rights. Where required by applicable law, the Bank ensures that such systems are always subject to human oversight, with the possibility to monitor, correct or override the recommendations generated automatically. Appropriate technical and organizational measures are also implemented to ensure the security, integrity and confidentiality of the data, which are safeguarded and protected through the Bank's controls and are not used for purposes other than those provided for.

6. Automated decision-making



The Bank uses automated systems to assess credit risk in the event of requests for the granting of credit (for example, if you apply for a loan) and during the management of existing relationships (European regulations require banks to continuously update credit risk assessments in order to ensure their stability and capital adequacy, also at banking group level). Credit risk analysis involves assigning a summary assessment (so-called "credit scoring"), obtained through the application of models and artificial intelligence systems that process data relating to the relationships you have with the Bank (for example, current account transactions), data contained in the documentation you provide (for example, income documentation) and information obtained from the consultation of databases. The models and statistical analysis factors, together with the algorithms used to calculate the assessments, the indicators and the scores, are subject to periodic review, human intervention is always provided to assess whether to confirm the granting of the requested product or service.

The Bank collects and analyzes in real time data relating to user behaviour and transactions in order to prevent, detect and monitor fraud risks in payment services; the personal data processed are those strictly necessary to ensure the accuracy of the analysis, the effectiveness of the systems used and their reliability over time. In order to identify suspicious activities, the Bank uses automated systems that make it possible to assign a summary assessment to determine whether the transactions can be attributed to the client, in order to intervene promptly where a concrete risk of fraud is detected. Behavioural analysis is also carried out using artificial intelligence systems, information obtained from the device used (for example, data from smartphone sensors) and predictive models based on statistical algorithms, which are periodically reviewed. The alerts generated by automated systems are reviewed by a dedicated anti-fraud team of the Bank, which verifies the legitimacy of the activity in suspicious cases, implementing any additional security measures and, in higher-risk cases, temporarily blocking the transactions.

7. Data recipients

The Bank may disclose personal data both to authorised persons (for example employees and collaborators) and to third parties who process such data in their capacity as data processors, joint controllers or independent data controllers. The Bank, without the need to obtain the client's consent, may communicate personal data to various categories of recipients, such as, for example:



- companies of the Banco BPM Group (such as, for example, Banca Akros, Banca Aletti, etc.), for the performance of administrative and service activities, including the sharing of data relating to suspicious transaction reports;
- entities operating within and outside the European Union (by way of example: credit institutions, payment systems and networks, consultants, professional firms, companies providing IT systems and services, companies providing market research and marketing services, insurance companies, debt collection agencies, consumer credit companies, leasing companies, etc.), which may process your data in their capacity as independent data controllers, data processors or joint controllers;
- judicial authorities, the Italian Revenue Agency, social security institutions, administrative and sector-specific authorities, public information systems, such as, for example, the Tax Register, the Central Credit Register at the Bank of Italy, the Central Anti-Fraud Office for Payment Means (the "UCAMP") and the Public System for the Administrative Prevention of Fraud in Consumer Credit, particularly in relation to identity theft (the "SCIPAFI"), as well as those entities to whom disclosure is required by law. These entities will process the data in their capacity as independent data controllers.

In order to carry out international financial transactions (for example, a cross-border transfer) and certain specific domestic transactions (for example, a high-value transfer) requested by clients or carried out in their favour, the Bank uses an international messaging service operated by SWIFT ("Society for Worldwide Interbank Financial Telecommunication", with registered office in Belgium). In the provision of these services, the Bank and SWIFT act as joint controllers, and the relevant privacy notice is available on the website www.bancobpm.it, in the Privacy section.

8. Transfers of data outside the EU



Your personal data are mainly processed within the European Union. The Bank will transfer personal data to countries outside the EU only where necessary for technical and organisational reasons; in any event, such processing will be carried out in compliance with the appropriate safeguards under applicable law, such as adequacy decisions adopted by the European Commission, standard contractual clauses approved by the European Commission, or other legal instruments.

9. Data retention



The Bank retains personal data for the period strictly necessary to achieve the purposes for which they were collected, in compliance with statutory limitation periods or with any different timeframes established by the applicable legislation or required for reasons of justice or public interest. For example, in order to comply with specific legal obligations, data may be retained for up to 10 years from the date of termination of the contractual relationship or from the date of execution of an occasional transaction.

10. Data subject's rights

In relation to your personal data, you may:



- obtain confirmation as to whether or not personal data concerning you exist and obtain a copy thereof in intelligible form;
- obtain the updating, rectification or completion of your data;
- request the erasure of your data, within the limits permitted by applicable law;
- object, in whole or in part, to the processing of personal data concerning you;
- obtain restriction of processing, in the event of unlawful processing, request for rectification or objection;
- request the portability of data processed by electronic means, where such data are provided on the basis of consent or a contract;
- withdraw your consent to the processing of your data, where applicable. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal;
- in relation to profiling based solely on automated processing, obtain human intervention from the Data Controller, express your point of view and contest the decision;

If you consider it appropriate, you may lodge a complaint with the Italian Data Protection Authority (“Garante per la Protezione dei Dati Personali”), in accordance with the procedures provided for by law. You can find all relevant information on the website www.garanteprivacy.it. To submit requests to the Bank free of charge, please visit the Privacy section of the website www.bancobpm.it, where you can download the relevant form and send it duly completed by email to protezionedati@bancobpm.it, via certified email (PEC) to protezionedati@pec.bancobpmspa.it, or by registered mail to the Bank’s registered office at Piazza F. Meda no. 4, 20121 Milan, “For the attention of the DPO – Data Protection Officer”. In order to protect its clients, the Bank may request information to verify your identity. We will respond within one month, except in complex cases (up to a maximum of three months). In any case, within one month we will inform you of the reason for the delay. You will receive a response in writing or in electronic format. If you request rectification, erasure or restriction of processing, we will inform the recipients of your data, unless this proves impossible or involves a disproportionate effort. We may refuse the request if it is manifestly unfounded or excessive, in particular due to its repetitive nature. For this purpose, we maintain a register to track your requests.

The icons used in this Privacy Notice are provided by the Maastricht European Centre on Privacy and Cybersecurity (ECPC) and have been developed as part of the “Informative chiare - Garante Privacy” initiative. The use and dissemination of this Privacy Notice are subject to the terms of the CC BY 4.0 licence (https://creativecommons.org/licenses/by/4.0/deed.it).

BANCO BPM

GRUPPO BANCO BPM