Ifis npl
Banca Ifis

PRIVACY POLICY

1. Introduction

Pursuant to Articles 13 and 14 of Regulation (EU) 2016/679 (the "Regulation"), IFIS NPL S.p.A. (the "Company" or "Data Controller"), as Data Controller, wishes to inform its customers, including potential customers, guarantors, coobligors and third-party payers, and third parties in general (e.g. attorneys, legal representatives, etc.) who come into contact with the Company as a representative or under customer mandate ("Data Subjects"), that their personal data ("Data") will be processed lawfully, correctly and transparently, in accordance with the methods and for the purposes shown below.

2. Sources of personal data

The Data to be processed by the Data Controller will be acquired, directly by the Company and/or via third-party entities duly appointed for the purpose, from Data Subjects and/or third parties (entities that perform transactions for the Data Subject, commercial and credit information companies, external market research companies, etc.), including through distance communication techniques which the Data Controller uses (e.g. websites, apps for smartphone and tablet, call centres, etc.). Data will also be used that are provided by public sources, such as public registers, lists, documents that can be accessed by the public (e.g. financial statements, information contained in business registers held by Chambers of Commerce, property deeds and other so-called adverse entries, such as registration of collateral or transcription of distraint proceedings, injunctions or other legal documents), and Data extracted from publicly accessible sources, such as newspapers or digital versions of newspapers, information available from telephone directories, and the websites of public bodies or other Regulatory authorities and control bodies.

3. Purpose and legal basis for processing

Data will be processed as part of the Data Controller's normal business activities, for the following purposes:

A) to fulfil legal obligations, both national and European, and obligations from orders/provisions from Public Authorities and/or Regulatory Bodies (e.g. obligations imposed by legislation to combat money laundering, terrorism, child pornography and tax evasion, etc.);

B) to fulfil obligations arising from a contract entered into with the Data Subject and/or that are necessary to enter into a contract, including managing and fulfilling specific requests from the Data Subject, and other activities which are connected and instrumental to the performance and management of the relationship (e.g. payment management; checks on the performance of the relationship, and its connected risks; etc.);

C) after receiving specific consent:

c.1) to identify the Data Subject's tastes, preferences, habits, needs and consumer choices (profiling) for direct marketing purposes;

c.2) to promote and supply the Company's products/services or to carry out market research aimed at determining the Data Subject's level of satisfaction;

c.3) to promote and supply third-party products/services;

c.4) to disclose personal data to third parties in order to promote and supply the Company's products/services or to carry out market research aimed at determining the Data Subject's level of satisfaction;

c.5) to disclose personal data to third parties in order for them to promote and supply their products/services;

D) to pursue the Data Controller's legitimate interests (e.g. protecting business assets; debt recovery; transferring credit or a contract concluded with the Data Subject; accounting and audit; credit monitoring; monitoring and assessment of the quality of service; managing disputes, lodging or defending a claim in and out of court; etc.).

With regard to the purposes under points A) and B), Data will be processed by the Data Controller, including concerning their communication to entities referred to in paragraph 7 and, within the limits in which this communication is functional to the pursuance of the related purposes, without the need for consent, given that the legal basis for processing is, respectively, to fulfil a legal obligation and perform a contract or to manage activities that are necessary to enter into a contract. If the Data Subject refuses to provide the necessary information, it will be impossible for the Data Controller to enter into a relationship with the Data Subject. With regards to the purposes under point C), the Data Subject has the right not to give consent, and to oppose, at any time, the performance of processing operations set out by the Data Controller, since the legal basis for processing is the Data Subject's consent. The only consequence of refusing to give consent is that the Data Subject will not be able to make use of the related services, without this leading to any negative consequences. Consent may be revoked at any time, without affecting the legitimacy of data processing already carried out. In relation to the purposes under point D), the Data Subject's consent is not necessary, since the legal basis for processing is the Data Controller's legitimate interests, taking into account the balance between the Data Controller's rights and those of the Data Subject.

4. **Categories of personal data**

The following categories of personal data may be processed for the purposes set out at paragraph 3: identification and contact data (e.g. name, surname, place and date of birth, e-mail address, tax reference number, profession and sector of activity, username and password used to access systems that the Data Controller makes available to the Data Subject, including mobile applications), and data relating to their connection with other entities; data relating to transactions (e.g. the amount and date of transactions, data identifying other banking relationships, IBAN number); financial data (e.g. statement of financial position and cash flow situation, payment history, creditworthiness); data that can identify tastes, preferences, life habits, and consumer choices. The Data Controller, limited to what is necessary to pursue the purposes set out at paragraph 3, may also become aware of and process criminal record data, as well as data that the Regulation defines as a special category of personal data (e.g. data revealing racial and ethnic origin, religious or philosophical beliefs, trade union membership, data concerning health or a natural person's sex life or sexual orientation), if these have been sent directly by the Data Subject.

5. Methods used to process personal data

Data are processed using manual, computerised and telematic tools, with approaches that are strictly linked to the purposes set out above and are, in any case, in compliance with the necessary care, guarantees and measures set out in the relevant legislative and regulatory provisions, aimed at ensuring the confidentiality, integrity and availability of Data, as well as avoiding damage, whether material or non-material (e.g. loss of control of personal data or limitation of rights, discrimination, identity theft or fraud, financial losses, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage).

The processing carried out by the Data Controller may be based on automated decision-making processes which have legal effect or which have similar significant effect on the Data Subject, including profiling: in particular, the Data Controller uses a partially-automated system aimed at profiling Data Subjects based on credit behaviour and adopting subsequent decisions on the profile generated as part of classification activities and bad debt reports regarding the Data Subject made to the Italian Central Risk Register. The Central Risk Register is an information system, managed by the Bank of Italy, that collects information provided by banks and financial institutions regarding credit granted to their customers and regarding the related guarantees and which provides an overview of all personal and business debts owed to the banking and financial system. This means that customers with a good credit history can obtain financing more easily and under better terms and conditions. Banks and financial institutions use it to assess a customer's ability to repay financing. Making bad debt reports regarding Data Subjects to the Central Risk Register may therefore have the effect of preventing a Data Subject from being granted financing. Statistical analysis models or factors, and the algorithms used to calculate judgements, indicators or scores that identify which positions require a bad debt report are prepared and updated in accordance with what is set out by the relevant legislative and regulatory provisions on the subject.

6. Transferring data to non-EU countries/organisations

Where it is necessary to achieve the purposes referred to in paragraph 3, a Data Subject's Data may be transferred abroad, to countries/organisations outside the EU which guarantee a level of personal data protection that the European Commission deems to be appropriate, or in any case based on other appropriate safeguards, for example, the Standard Contractual Clauses adopted by the European Commission.

A copy of any Data transferred abroad, as well as the list of non-EU countries/organisations to which Data have been transferred, may be requested from the Data Controller using the contact details indicated in paragraphs 9 and 10.

7. Categories of entity to which personal data may be disclosed or which may become aware of these data

To pursue the purposes described in paragraph 3, the Data Controller reserves the right to disclose Data to the following categories of recipient:

- Regulatory Authorities and Control Bodies and, in general, public entities or private entities performing a public role (e.g. the Bank of Italy's Financial Intelligence Unit, the Bank of Italy, the Agenzia delle Entrate [Italian Tax Agency], the Interbank Register of Bad Cheques and Payment Cards, the Bank of Italy's Central Credit Register, law enforcement agencies, in any case only where the conditions established by the applicable legislative and regulatory provision have been met);
- Public Bodies (economic and territorial) and Public Administration;
- other companies of the Group to which the Company belongs, whether parent, subsidiary or associated, pursuant to Article 2359, Italian Civil Code (including where these are located abroad);
- companies managing national and international systems combating fraud against banks and financial intermediaries;
- entities responsible for checking, auditing and certifying the Company's activities;
- entities which carry out banking, financial and insurance services;
- trade associations;
- companies which compare the Data provided by the Data Subject with those available on public registers, lists, deeds or documents available to the general public, in order to verify if these data are correct, also to fulfil due diligence obligations imposed by the Anti-Money Laundering Decree, as well as in cases of protests and adverse entries;
- entities carrying out data collection, processing and study services;
- entities providing IT management services for the Data Controller and services for the management of the telecommunications network (including mailing services);
- entities which print, envelope, transmit, transport and sort communications;
- entities responsible for document storage and data-entry;
- entities responsible for providing customer service activities to the Data Subject;
- professional firms or companies providing assistance and consultancy services (e.g. accountancy firms, law firms, etc.);
- companies that perform credit assessments, credit risk and insolvency reports, over-indebtedness prevention and credit protection activities, including credit information systems;
- financial agents, loan brokers and other intermediaries operating in the credit, financial or banking sector, including debt collection agencies, with the role of managing the Company's products and/or services;
- entities providing the Interbank Corporate Banking (CBI) service;
- entities carrying out communication assistance and consultancy activities (e.g. market research activities aimed at identifying the level of satisfaction expressed by Data Subjects on the quality of the services provided and activities carried out by the Company, telemarketing etc.);
- coobligors, guarantors and third-party payers;
- entities which, in various roles, succeed the Company in ownership of legal relationships (e.g. assignees or potential assignees of assets, receivables and/or contracts).

The entities belonging to the categories listed above operate independently as separate Data Controllers, or as Data Processors appointed for this purpose by the Company. A list of these entities, which is constantly updated, is available at www.bancaifis.it. Data may also become known, in the performance of assigned tasks, by the Data Controller's personnel, including interns, temporary workers, consultants, all of whom are appropriately authorised to process personal data. Personal data will not, in any case, be publicly disclosed and, therefore, will not be made available to or be consulted by unauthorised entities/individuals, in any form.

8. Storage and erasure of personal data

Pursuant to Article 5, paragraph 1, letter e) of the Regulation, Data will normally be held in a form that enables identification of Data Subjects for no longer than is necessary for the purposes for which the personal data were collected and processed, in accordance with the principle of proportionality and necessity set out in legislation on protection of personal data. In determining the storage period, laws applying to the activities and the sectors in which the Data Controller operates will also be considered (e.g. Anti-Money Laundering law and laws which govern the keeping of accounting records), as well as Garante's [Italian Data Protection Authority] general and special provisions regarding the protection of personal data (e.g. in relation to storage periods for marketing and profiling purposes). When this deadline expires, Data will be erased or anonymised, except where they must be further stored to fulfil legal obligations or to carry out orders given by Public Authorities and/or Regulatory Bodies.

9. A Data Subject's rights

In accordance with Articles 15 to 22, the Regulation allows Data Subjects to exercise specific rights. In particular, Data Subjects may obtain: a) confirmation of the existence of personal data processing which concerns them and, where that is the case, access to those personal data; b) rectification of inaccurate personal data and to have incomplete personal data completed; c) the erasure of personal data which concern them, where permitted by the Regulation; d) the restriction of processing, in the cases provided for by the Regulation; e) the communication of any requests from the Data Subject for rectification or erasure of personal data or restriction of processing to be sent to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort; f) to receive the personal data which they have provided to the Data Controller, in a structured, commonly used and machine-readable format and the right to transmit those data to another Data Controller, at any time, even where the relationship established with the Data Controller has ceased. Data Subjects also have the right to oppose, at any time, the processing of personal data concerning them: in this case, the Data Controller is obliged to refrain from any further processing, except for the scenarios set out in the Regulation. Data Subjects also have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or has a similar effect on them, unless this decision is: a) necessary for entering into or performing a contract between the Data Subject and a Data Controller; b) authorised by European Union law or Member state law to which the Data Controller is subject; c) based on the Data Subject's explicit consent. In the cases specified in points a) and c) above, Data Subjects have the right to obtain human intervention from the Data Controller, to express their opinion and to appeal against the decision.

These requests may be submitted to the organisational unit responsible for responding to Data Subjects, by sending a letter to the headquarters of the Data Controller, or by e-mail to privacy@bancaifis.it.

Data Subjects also have the right to lodge a complaint with Garante [Italian Data Protection Authority], as set out in Article 77 of the Regulation, and to effective judicial remedy in accordance with Articles 78 and 79 of the Regulation.

10. Data Controller and Data Protection Officer

The Data Controller is IFIS NPL S.p.A., with registered office in Venice – Mestre, Via Terraglio no. 63. The Data Controller has appointed a Data Protection Officer, who can be contacted by email at: rpd@bancaifis.it.

PRIVACY POLICY ON THE RECORDING OF TELEPHONE CALLS

The Company wishes to inform its borrowers that it uses a system to record telephone calls as part of its activities relating to:

- debt collection and telephone contact carried out by debt collection agencies, in their role as Data Processor, installed exclusively for the purposes of monitoring the quality of the service made available to the user. Recordings are stored with restricted access and are held at the debt collection agency's offices only for the time strictly necessary to achieve the purposes for which they were made. In any case, the maximum storage period cannot exceed 12 months;
- management of debt acknowledgement and extension agreements by the Contact Center. These recordings will be kept confidential and stored in the substitute storage system pursuant to law for 10 years from the moment in which their effects expire.

Telephone calls are recorded using automated systems which record outgoing and incoming calls. Appropriate measures are taken to guarantee the security and confidentiality of the collected data, as set out by current legislative and regulatory provision on the protection of personal data. Telephone call recordings can be accessed by persons expressly authorised to process personal data, in order to protect the Company's workers and business assets from direct or indirect damage which may result from claims raised by customers, to monitor the quality of the service made available to the user, to fulfil internal audit obligations as set out by legislative and regulatory provisions to guarantee that customers and/or business assets are protected and to satisfy requests from external control bodies (Consob [Supervisory Authority for the Italian financial products market], Bank of Italy, external auditor, etc.), that are legally allowed to access telephone call recordings in their role as independent Data Controllers.

INFORMATION PURSUANT TO ARTICLE 6 OF THE CODE OF CONDUCT FOR INFORMATION SYSTEMS MANAGED BY PRIVATE ENTITIES WITH REGARD TO CONSUMER CREDIT AND CREDITWORTHINESS

How we use your data

This information as referred to in Articles 13 and 14 of Regulation (EU) 2016/679 has also been drafted on behalf of credit information systems.

Dear Customer,

IFIS NPL S.p.A., in its role as Data Controller, would like to inform you that, to respond to your request, it uses some data that concern you. This is information you provide to us or that which we obtain by consulting databases.

These databases ("Credit Information Systems" or "CIS") containing information regarding Data Subjects are consulted to assess, assume or manage credit risk, and to assess a Data Subject's creditworthiness. The databases are managed by private entities and are contributed to by private entities belonging to the categories which you will find in the privacy policy provided by the managers of the CIS.

This information will be stored on our premises; some of the information you provide us, together with information regarding your payment behaviour as part of the relationship that will be established may be communicated periodically to the CIS.

This means that the entities belonging to the categories mentioned above, with whom you have requested to establish a relationship, may know if you have submitted a request to us and whether or not you make regular payments.

Processing and communication of your data is a necessary requirement for entering into a contract. Without these data, we may not be able to respond to your request.

Banks store this information as part of a Data Controller's legitimate interests in consulting CIS.

Processing carried out by the Company

Your Data may be subject to transfer to a non-EU country or international organisation, in accordance with the methods set out in paragraph 6 of the privacy policy above.

In accordance with the terms, methods and limits of applicability established by current legislative and regulatory provisions, you have the right to receive information regarding your data and to exercise various rights relating to their use (rectification, update, erasure, limitation of processing, opposition, etc.).

You may lodge a complaint with Garante [Italian Data Protection Authority] (www.garanteprivacy.it), and use other means of protection set out in applicable legislative and regulatory provisions.

We store your data on our premises for the period of time necessary to manage your contractual relationship with us and to fulfil legal obligations (e.g. with regard to what is set out in Article 2220, Italian Civil Code, regarding the keeping of accounts).

For any request regarding your data, you can write to this Company at privacy@bancaifis.it and/or to the companies indicated below to which we will communicate your data.

Your data may not be used in an automated decision-making process for a request, in the event that this decision is necessary to enter into or perform your contract with us.

We would also like to notify you that if for any reason you wish to contact our Data Protection Officer, you can do so at rpd@bancaifis.it.

Processing carried out by managers of CIS

In order to better assess creditworthiness, we will communicate some data (personal details, including of any coobligor, type of contract, amount of credit, method of repayment) to Credit Information Systems, which are regulated by the relevant Code of Conduct and which are independent Data Controllers. Data are also made available to various private entities belonging to the categories which you will find in the privacy policy provided by the managers of CIS, available through the channels listed below.

Data concerning you are periodically updated with information acquired over the course of the relationship (payment performance, residual debt exposure, status of the relationship).

As part of the work done by CIS, your data will be processed in accordance with the methods of organisation, comparison and studies that are strictly necessary to pursue the purposes described above.

Your data are subject to statistical studies in order to give you a score regarding your creditworthiness (credit scoring). These studies take into consideration some principal factors which include, but are not limited to: the number and characteristics of existing credit relationships, payment performance and history for existing or extinguished credit relationships, if there are new requests for credit and, if so, their characteristics, history of extinguished credit relationships, whether or not there are any adverse data, etc., which enable us to obtain, by applying statistical methods and models, results expressed as a summary opinion, numerical indicators or scores, aimed at providing a prediction or probable representation of a Data Subject's creditworthiness.

Some additional information may be provided to you if a credit application is not accepted.

The CIS we use are managed by:

IDENTIFICATION DETAILS: Experian Italia S.p.A.

CONTACT DATA: registered office in Piazza dell'Indipendenza no. 11/b, 00185 Rome; Consumer Protection Service: tel.: 199183538 fax: 199101850; Data Protection Officer: dpoItaly@experian.com; website: www.experian.it

TYPE OF SYSTEM: positive and negative

DATE STORAGE PERIODS: these periods are indicated in the table below

USE OF AUTOMATED CREDIT SCORING SYSTEMS: yes

IS THERE AN AUTOMATED DECISION-MAKING PROCESS?: no

You have the right to access data concerning you at any time. Please contact our Company, sending your request to privacy@bancaifis.it, or to the managers of CIS, using the details indicated above.

In the same way, you may request rectification, updating or supplementation of inaccurate or incomplete data, or the erasure or blocking of personal data processed in violation of the law, or you may also object to their use for legitimate reasons to be outlined in the request (Articles 15 to 22 of Regulation (EU) 2016/679, excluding Article 20).

Periods of data storage in CIS

financing requests	not more than 180 days from the date of application, if the request is accepted not more than 90 days from the date of monthly update, if the request is not accepted or is withdrawn
rectified delays no greater than two instalments or two months	up to 12 months from rectification
rectified delays greater than two instalments or two months	up to 24 months from rectification
unrectified delays or breaches	not more than 36 months from the contractual due date of the relationship or from the date on which the latest update was made necessary, and in any case not more than 60 months from the contractual due date of the relationship
relationships that are extinguished with extinction of all pecuniary obligations	not more than 60 months from the date of termination of the relationship or the due date of the related contract, or from the first update carried out in the month following those dates more than 60 months, if there are unrectified delays or breaches relating to other credit relationships