DATA PROTECTION NOTICE

Last updated April 2025

Introduction

We take the protection of your personal data very seriously; accordingly, the BNP Paribas Group has adopted strong principles in its Personal Data Protection Notice available at https://group.bnpparibas/protection-donnees

FLOA ("**We**"), as a controller, is responsible for collecting and processing your personal data in relation to its activities.

Our business is to help all our customers – individuals – in their day-to-day banking activities and in achieving their projects thanks to our financing.

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

The purpose of this Privacy Notice is to explain how we process your personal data and how you can control and manage them.

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

1. ARE YOU SUBJECT TO THIS NOTICE?

This Privacy Notice applies to you if you are ("**You**"):

- one of our customers or in a contractual relationship with us ;
- a member of our customer family. Indeed, our customers may occasionally share with us information about their family when it is necessary to provide them with a product or service or to get to know them better;
- a person interested in our products or services when you provide us with your personal data (on our websites and applications, on social networks, during events or sponsorship operations) so that we can contact you.

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 Privacy Notice. 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 CONTROL THE PROCESSING ACTIVITIES WE DO ON YOUR PERSONAL DATA?

You have rights which allow you to exercise real control over your personal data and how we process them.

We draw your attention to the fact that these rights may be limited where regulations so provide. This is the case with the regulations relating to the fight against money laundering and the financing of terrorism, which prohibit us from allowing you to exercise your various rights with regard to your personal data processed for this purpose. In this case, you must exercise your right of access with the supervisory authority of your country, which will request the data from us.

If You wish to exercise the rights listed below, please submit a request :

- by mailing a letter to the following address : Service consommateur – FLOA – 36 rue de Messines – 59 686 Lille Cedex 9 or
- by email to the following address: crc@services.floa.fr

Where We have reasonable doubts, We may request the provision of additional information necessary to confirm Your identity.

If you have any questions relating to our use of your personal data under this Privacy Notice, please contact our Data Protection Officer at the following address dpo@floa.com.

2.1. You can request access to your personal data

You can directly access some data from your client account on our website www.floapay.it or via the FLOA mobile applications (if available).

If you wish to have access to your personal data, we will provide you with a copy of the personal data you requested as well as information relating to their processing.

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

Where you consider that your personal data are inaccurate or incomplete, you can request that such personal data be modified or completed accordingly. In some cases, supporting documentation may be required.

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 the 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 marketing purposes

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

2.6. You can suspend the use of your personal data

If you question the accuracy of the personal data we use or object to the processing of your personal data, we will verify or review your request. You may request that we suspend the use of your personal data while we review your request.

2.7. You have rights against an automated decision

As a matter of principle, you have the right not to be subject to a decision based solely on automated processing based on profiling or otherwise that has a legal effect or significantly affects you. However, we may automate such a decision if it is necessary for the entering into or performance of a contract with us, authorised by regulation or if you have given your consent.

In any event, you have the right to challenge the decision, express your views and 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 Italian Data Protection Authority

In addition to the rights mentioned above, you may lodge a complaint with the competent supervisory authority, which is usually the one in your place of residence, in Italy the Italian Data Protection Authority (Garante per la Protezione dei Dati Personali).

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 are processed to comply with our various legal obligations to which we are subject

Your personal data are processed where necessary to enable us to comply with the 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 identify those which deviate from the normal routine/patterns;
- manage and report risks (financial, credit, legal, compliance or reputational risks etc.) that the BNP Paribas Group could incur in the context of its activities;
- record, in compliance with the regulations relating to distance selling when apply, communications in any form relating to products or services purchased;
- assist the fight against tax fraud and fulfil tax control and notification obligations;
- when mandatory, record transactions for accounting purposes;
- prevent, detect and report risks related to Corporate Social Responsibility and sustainable development;
- detect and prevent bribery;
- when applicable, comply with the provisions applicable to trust service providers issuing electronic signature certificates;
- exchange and report different operations, transactions or orders or reply to an official request from a duly authorized local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, law enforcement, state agencies or public bodies;

  respond to requests relating to the exercise of your rights, addressed to FLOA in accordance with **article 2**.

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.

In this context, we 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 carried out under joint controllership and performed to meet these legal obligations are detailed in **Appendix 1**.

3.2. Your personal data are processed to perform a contract to which you are a party or pre-contractual measures taken at your request

Your personal data are processed when it is necessary to enter into or perform a contract to:

- define your credit risk score and your reimbursement capacity ;
- evaluate (e.g., on the basis of your credit risk score) if we can offer you a product or service and under which conditions ;
- provide you with the products and services subscribed to under the applicable contract;
- keep proof of operations or transactions, including in electronic format;
- manage existing debts (identification of customers in arrears) including payment incidents, overdue payments and amicable or judicial recovery of any credit granted.
- respond to your requests and assist you;
- ensure the settlement of your succession;
- take into account your registration for the competitions organised by or in partnership with FLOA, manage your participation, enter You in the prize draws and send You your winnings, where applicable.

3.3. Your personal data are 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 or 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 at the following address: Service consommateur – FLOA – 36 rue de Messines – 59 686 Lille Cedex 9 or at dpo@floa.com email address.

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

- manage the risks to which we are exposed:
  - when mandatory, we keep proof of operations or transactions, including in electronic evidence;
  - we monitor your transactions to manage, prevent and detect fraud;
  - we handle legal claims and defences in the event of litigation;
  - we develop individual statistical models in order to help define your creditworthiness;
- enhance cyber security, manage our platforms and websites, and ensure business continuity;
- use video surveillance to prevent personal injury and damage to people and property;
- enhance the automation and efficiency of our operational processes and customer services (e.g., automatic filling of forms, 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);
- assist you in managing your budget by automatic categorization of your transaction data;
- If necessary, carry out financial operations such as debt portfolio sales, securitizations, financing or refinancing of the BNP Paribas Group.
- conduct statistical studies and develop predictive and descriptive models for:
  - commercial purpose: to identify the products and services that could best meet your needs, to create new offers or identify new trends among our customers, to develop our commercial policy taking into account our customers' preferences
  - safety purpose: to prevent potential incidents and enhance safety management;
  - compliance purpose (e.g., anti-money laundering and countering the financing of terrorism) and risk management;
  - anti-fraud purposes.
- organize promotional operations, conduct opinion and customer satisfaction surveys.

3.3.2. We use your personal data to send you commercial offers by electronic means

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.

Once you are a customer and unless you object, we may send you these offers by electronic meansfor our products and services and those of the Group, if they are similar to those you have already subscribed to.

We will ensure that these commercial offers relate to products or services that are relevant to your needs and complementary to those you already have to ensure that our respective interests are balanced.

We may also send you, by phone and post, unless you object, offers concerning our products and services as well as those of the Group and of our partners.

3.3.3. We analyse your personal data to perform standard profiling to personalize our products and offers

To enhance your experience and satisfaction, we need to determine to which customer group you belong. For this purpose, we build a standard profile from relevant data that we select from the following information:

- what you have directly communicated to us during our interactions with you or when you subscribe to a product or service;

- resulting from your use of our products or services such as those related to your accounts including the balance of the accounts, regular or atypical movements, the use of your card abroad as well as the automatic categorization of your transaction data (e.g., the distribution of your expenses and your receipts by category merchants (e.g. purchases made from a travel retailer));
- from your use of our various channels: websites and applications (e.g., if you are digitally savvy, if you prefer a customer journey to subscribe to a product, or service with more autonomy (selfcare));

Unless you object, we will perform this customization based on standard profiling. We may go further to better meet your needs, if you consent, by performing a tailor-made customization as described below.

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

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

In particular, we ask for your consent for:

- tailor-made customization of our offers and products or services (as detailed in **Appendix 2**);
- Any electronic offer for products and services not similar to those you have subscribed to or for products and services from our trusted partners;
- personalization of our offers, products and services based on your account data at other banks;
- use of your navigation data (cookies) for commercial purposes or to enhance the knowledge of your profile in accordance with our Cookie Management 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 allows one 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., civil status, full name, gender, place and date of birth, nationality, identity document number (identity card, passport), photograph, digital selfie, signature);
- **Contact information**: postal address, e-mail address, landline and mobile phone number;
- **Information relating to your financial and family situation**: e.g., marital status, matrimonial regime, number of children and age, composition of the household, property you own: apartment or house;
- **Milestones of your life**: e.g., you recently got married, divorced, partnered, or gave birth;
- **Economic, financial and tax information:** e.g., country of residence, salary and other income, expenses;
- **Education and employment information:** e.g., employment, seniority, employer's name and remuneration;
- **Banking and financial information related to the products and services you hold / requested**: e.g., bank account details (RIB/IBAN, bank card number, expiry date of bank card), bank establishment, seniority, products and services requested / owned and used (credit, home protection), amount and duration of products or services requested/held and used schedules, credit history, history of the products and services to which You have subscribed or to which You have asked to subscribe, payment incidents;
- **Transaction data:** file number corresponding to the products and services that You hold/requested, account movements and balances, transactions including beneficiary's data such as full names, addresses and contact details as well as details of bank transactions, amount, date, time and type of transaction (credit card, transfer, cheque, direct debit);
- **Data relating to your habits and preferences in relation to the use of our products and services**;
- **Data collected from our interactions with you**: e.g., your comments, suggestions, needs collected during our exchanges with you and online during phone communications (conversation), discussion by e-mail, chat, chatbot, exchanges on our social media pages and your latest complaints and your connection, navigation and tracking data such as cookies and tracers for non-advertising or analytical purposes on our websites, online services, applications, social media pages in accordance with our Cookie Management Policy;
- **Data about your devices (mobile phone, computer, tablet, etc.)**: IP address, technical specifications and uniquely identifying data;
- **Personalized login credentials or security features used to connect you to FLOA websites 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.

5. WHO DO WE COLLECT PERSONAL DATA FROM?

We collect personal data directly from you; however, we may also collect personal data from other sources.

We sometimes collect data from public sources:

- publications/databases made available by official authorities or third parties (e.g. 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 third parties:

- from other BNP Paribas Group entities;
- from our customers (companies or individuals);
- from the from our business partners; third parties with whom You have subscribed to a product or service and/or whom You have authorised to communicate your personal data to Us;
- from credit information systems ("SICs"), as mentioned in **Annex 2**;
- from service providers of payment initiation and account aggregators (service providers of account information);
- from third parties such as credit reference agencies and fraud prevention agencies;
- from data brokers who are responsible for ensuring that they collect relevant information in a lawful manner.

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 BNP Paribas Group entities, where necessary, to:

- comply with our various legal and regulatory obligations described above;
- fulfil our legitimate interests which are:
    - to manage, prevent, detect fraud;
        - conduct statistical studies and develop predictive and descriptive models for business, security, compliance, risk management and anti-fraud purposes;
    - enhance the reliability of certain data about you held by other Group entities;
    - offer you access to all the Group's products and services that best meet your needs and wishes;
    - customize the content and prices of products and services.

b. With recipients outside the BNP Paribas Group and processors

In order to fulfil some of the purposes described in this Privacy Notice, we may, where necessary, share your personal data with:

- processors which perform services on our behalf (e.g., IT services, logistics, printing services, telecommunication, debt collection, advisory and distribution and marketing) as well as with the audit firms that support our business.
- 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 obligations or transaction (e.g., banks, correspondent banks, , payment system operators, issuers or payment card intermediaries);
- credit information systems ("SICs"), as mentioned in **Annex 2**;

- local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, public authorities or institutions (e.g., the *Banque de France*, *Caisse des dépôts et des Consignations*), 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 applying to us or any member of the BNP Paribas Group;
- service providers of third-party payment (information on your bank accounts), for the purposes of providing a payment initiation or account information service if you have consented to the transfer of your personal data to that third party;
- certain regulated professions such as lawyers, bailiffs, notaries, or auditors 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 BNP Paribas Group.

7. INTERNATIONAL TRANSFERS OF PERSONAL DATA

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, your personal data may be transferred on this basis.

For transfers to non-EEA countries where the level of protection has not been recognized as adequate by the European Commission, we will either rely on a derogation applicable to the specific situation (e.g., if the transfer is necessary to perform our contract with you, such as when making an international payment) or implement one of the following safeguards to ensure the protection of your personal data:

- Standard contractual clauses approved by the European Commission;
- Binding corporate rules.

To obtain a copy of these safeguards or details on where they are available, you can send a written request as set out in dpofloa@floa.com.

8. HOW LONG DO WE KEEP YOUR PERSONAL DATA?

We retain your personal data for the following periods:

- If you are one of our customers (a hypertext link links you to us), your personal data is kept for 5 years from the end of your contract and from the closure of your customer account.
- Your contract is kept for 10 years, in accordance with our legal obligations.
- If you are one of our prospective customers (you do not have a contract with us), your personal data is kept for 3 years from the date of collection or the last contact from you.
- If Your application for credit is unsuccessful, your personal data is kept for 6 months from the date of refusal of Your application.
- Special case of fraud alerts and blatant fraud :

o In the case of a fraud alert: any external fraud alert that is not qualified within 12 months of being issued is deleted immediately;
o o In the event of hard-core fraud: data relating to hard-core fraud is kept for a maximum of 5 years from the closure of the fraud file.

Data relating to persons registered on a list of proven fraudsters is deleted after a period of 5 years from the date of registration on the list.

- Recordings of telephone calls: these are kept for as long as is necessary to achieve the purpose for which they were made.

For example, in order to enhance the automation and efficiency of our operational processes and customer services, part of our telephone exchanges may be kept for the maximum duration of six months (except if you object).

We draw your attention to the fact that some telephone recordings are made by us on behalf of our partners and that, in such a case, it will be up to the partner to inform Us of your request to exercise your rights.

- Cookies and tracers: the procedures for depositing cookies and other tracers are detailed in our dedicated Policy.

When an amicable, administrative or legal procedure is in progress, your personal data is kept until its conclusion. It is then archived in accordance with the applicable legal statute of limitations. You will be informed of any processing of personal data with a retention period other than those listed above.

Barring legal exceptions, You have the rights to your personal data detailed in **article 2**.

9. HOW TO FOLLOW THE EVOLUTION OF THIS PRIVACY NOTICE

In a world where technologies are constantly evolving, we regularly review this Privacy 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.

Appendix 1

Processing of personal data to combat money laundering and the financing of terrorism

We are part of a banking Group that must adopt and maintain a robust anti-money laundering and countering the financing of terrorism (AML/CFT) programme for all its entities managed at central level, an anti-corruption program, as well as a mechanism to ensure compliance with international Sanctions (i.e., any economic or trade sanctions, including associated laws, regulations, restrictive measures, embargoes, and asset freezing measures that are enacted, administered, imposed, or enforced by the French Republic, the European Union, the U.S. Department of the Treasury's Office of Foreign Assets Control, and any competent authority in territories where BNP Paribas Group is established).

In this context, we act as joint controllers together with BNP Paribas SA, the parent company of the BNP Paribas Group (the term "we" used in this appendix therefore also covers BNP Paribas SA).

To comply with AML/CFT obligations and with international Sanctions, we carry out the processing operations listed hereinafter to comply with our legal obligations:

- A Know Your Customer (KYC) program reasonably designed to identify, verify and update the identity of our customers, including where applicable, their respective beneficial owners and proxy holders;
- Enhanced due diligence for high-risk clients, Politically Exposed Persons or "PEPs" (PEPs are persons defined by the regulations who, due to their function or position (political, jurisdictional or administrative), are more exposed to these risks), and for situations of increased risk;
- Written policies, procedures and controls reasonably designed to ensure that the Bank does not establish or maintain relationships with shell banks;
- A policy, based on the internal assessment of risks and of the economic situation, to generally not process or otherwise engage, regardless of the currency, in activity or business:
    - for, on behalf of, or for the benefit of any individual, entity or organisation subject to Sanctions by the French Republic, the European Union, the United States, the United Nations, or, in certain cases, other local sanctions in territories where the Group operates;
    - involving directly or indirectly sanctioned territories, including Crimea/Sevastopol, Cuba, Iran, North Korea, or Syria;
    - involving financial institutions or territories which could be connected to or controlled by terrorist organisations, recognised as such by the relevant authorities in France, the European Union, the U.S. or the United Nations.
- Customer database screening and transaction filtering reasonably designed to ensure compliance with applicable laws;
- Systems and processes designed to detect and report suspicious activity to the relevant regulatory authorities;
- A compliance program reasonably designed to prevent and detect bribery, corruption and unlawful influence pursuant to the French "*Sapin II*" Law, the U.S FCPA, and the UK Bribery Act.

In this context, we make use of:

- services provided by external providers that maintain updated lists of PEPs such as Dow Jones Factiva (provided by Dow Jones & Company, Inc.) and the World-Check service (provided by REFINITIV, REFINITIV US LLC and London Bank of Exchanges);
- public information available in the press on facts related to money laundering, the financing of terrorism or corruption;
- knowledge of a risky behaviour or situation (existence of a suspicious transaction report or equivalent) that can be identified at the BNP Paribas Group level.

We carry out these checks when you enter into a relationship with us, but also throughout the relationship we have with you, both on yourself and on the transactions you carry out. At the end of the relationship and if you have been the subject of an alert, this information will be stored in order to identify you and to adapt our controls if you enter into a new relationship with a BNP Paribas Group entity, or in the context of a transaction to which you are a party.

In order to comply with our legal obligations, we exchange information collected for AML/CFT, anti-corruption or international Sanctions purposes between BNP Paribas Group entities. When your data are exchanged with countries outside the European Economic Area that do not provide an adequate level of protection, the transfers are governed by the European Commission's standard contractual clauses. When additional data are collected and exchanged in order to comply with the regulations of non-EU countries, this processing is necessary for our legitimate interest, which is to enable the BNP Paribas Group and its entities to comply with their legal obligations and to avoid local penalties.

Appendix 2

Automated decisions including profiling

We carry out various types of profiling, the characteristics of which are described below. Some or all of this profiling may be carried out in a fully automated manner, in accordance with **Article 2.7**.

1. Modelling and implementation of scoring rules for marketing purposes

The modelling of scoring rules for marketing purposes enables FLOA to find out its customers' and prospects' appetite for a product or service and their preferences, in particular as regards the communication channel used. FLOA can thus adapt its offer (product or service proposed and characteristics of the offer) and the frequency of contact.

The data taken into account for the determination of score models may be all the data concerning You, whether collected directly or indirectly. We select certain fields that are useful for modelling scoring rules for marketing purposes, which can be correlated with one or more others and then associated with a weighting.

Score rules modelled in this way can be used to :

- establish segments and categories of customers and prospects (e.g. based on behaviour observed when applying for a loan) ;
- identify the appetite of customers and prospects for a product or service;
- measure the reactivity of customers and prospects when they receive and open an offer sent by email / SMS and identify the preferences of customers and prospects with regard to the communication channel used.

FLOA may thus adapt its offers (products or services proposed and characteristics of the offers), the rhythm and the channel of communication in order to respect the choices of its customers and prospects, provide them with quality information and services, adapted to their needs, and improve their satisfaction.

This purpose may have the effect of excluding certain persons from marketing campaigns and/or certain communication channels.

2. Modelling and implementing scoring rules for granting and collection purposes

The modelling of scoring rules for granting and collection purposes enables FLOA to control credit risk (in the case of prospects) and non-payment risk (in the case of customers).

The data taken into account for the determination of score models may be all data concerning you, whether collected directly or indirectly. We select certain fields that are useful for modelling scoring rules for granting and collection purposes, which can then be correlated with one or more others and associated with a weighting.

In order to better assess the credit risk score, We communicate certain data (personal data, type of contract, amount of credit, repayment methods) to credit information systems ("**SIC**"), which are governed by the relevant SIC Code of Conduct approved by the Italian Data Protection Authority with Provision no. 163 of 19 September 2019.

These systems are large databases set up to assess credit risk, managed by private individuals and available to many parties.

This means that other banks or financial institutions from which the interested party will ask for another loan, financing, credit card, etc., even to buy a consumer good in installments, will be able to know if he has submitted a recent loan request to us, if he has other loans or financing in progress and if he regularly pays the installments.

For the purposes of concluding the contract and for the purposes of credit protection, creditworthiness assessment as well as for the prevention of over-indebtedness, the loan request submitted by you to us will also be subject to an automated decision-making process based exclusively on the data you provide, on the so-called credit scoring and on any information present in the SICs.

This process may result in the automatic acceptance or rejection of the funding request submitted. In any case, you will always have the right to obtain human intervention in order to be able to express your opinion or contest the decision. The SIC to which We adhere is managed by:

CRIF S.p.A.: with registered office in Bologna, Public Relations Office: Via Zanardi, no. 41, 40131 Bologna, Fax: 0516458940, Tel: 0516458900, website www.crif.it, positive and negative SIC, which includes, as categories of participants: banks, financial intermediaries, private individuals who, in the exercise of a commercial or professional activity, grant deferrals of payment of the consideration for the supply of goods or services.

Score rules modelled in this way can be used to calculate the credit risk (in the case of prospects) and non-payment risk (in the case of customers), enabling the person concerned to :

- subscribe to a product suited to their borrowing capacity ;
- prevent the risk of debt collection/over-indebtedness;
- be protected, in the case of customers identified as "fragile".

This purpose may have the effect of excluding certain people from taking out a loan (refusal to grant), leading to a change in the maximum loan amount or generating the proposal of a product more suited to the borrowing capacity of the person concerned.

3. Modelling and implementing scoring rules to combat fraud

Modelling score rules to combat fraud enables FLOA to identify signals that may help detect fraud, such as the technical and behavioural environments conducive to the action of a potential fraudster.

The data taken into account for the determination of score models can be any data concerning you, whether collected directly or indirectly. We select certain fields that are useful for modelling score rules to combat fraud, which can then be correlated with one or more others and associated with a weighting.

The implementation of score rules modelled in this way enables FLOA to :

- prevent fraudulent behaviour
- detect fraudulent behaviour
- combat fraudulent behaviour.

This may result in the exclusion of certain individuals from taking out a loan (refusal to grant), the termination of current contractual relations or the initiation of amicable or legal proceedings.