Banca Ifis

PRIVACY POLICY

1. Introduction

In accordance with Articles 13 and 14 of EU Regulation 2016/679 (the "Regulation"), Banca Ifis S.p.A. (the "Bank" or "Data Controller"), as Data Controller, wishes to inform its customers, including potential customers, guarantors, co-obligors and third-party payers, and third parties in general (e.g. attorneys, legal representatives, etc.) who come into contact or may come into contact with the Bank 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.

If the Data Subject is a legal person, the following information is also provided with regard to the personal data of natural persons who legally and / or organically represent it, of which the Data Controller becomes aware.

2. Sources of personal Data

The Data to be processed by the Data Controller will be acquired, directly by the Bank 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.). This will include the use of 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 is provided by public sources, such as public registers and 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 prejudicial documents, 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 orders/provisions from Public and/or Regulatory Authorities (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. credit assessment; payment management; checks on the performance of the relationship, and its connected risks; securitisation of credits; credit insurance; payment transactions, including international transactions, such as, cross-border bank transfers, for which it is necessary to use the SWIFT international messaging service, 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 (only where the Data Subject is a natural person);

c.2) to promote and supply banking 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 Bank'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; accounting and audit; credit monitoring; monitoring and assessment of the quality of service; managing disputes, that is 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 the contract or to manage activities that are necessary for the purposes of entering into a contract. If the Data Subject refuses to provide the necessary information, it will be impossible for the Data Controller to enter into the 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 Data Controller performing the processing operations set out, 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 having any negative effect on 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 of the Data Controller's rights with 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, user name 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 persons; data relating to transactions (e.g. current account number, deposits and withdrawals, 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, financial trustworthiness and punctuality of payment); data that can identify tastes, preferences, habits, needs and consumer choices; criminal record data. The Data Controller, limited to what is necessary to pursue the purposes set out at paragraph 3, may become aware of and process 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, as well as genetic data, biometric data, data concerning health or data concerning 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 an approach that is strictly linked to the purposes set out above and, in any case, in compliance with the necessary care, guarantees and measures prescribed by 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 adopts an automated system aimed at profiling Data Subjects based on credit behaviour and adopting subsequent decisions on the profile generated as part of the credit assessment process connected with a credit application (credit scoring) and a partially-automated system aimed at profiling Data Subjects based on credit behaviour and adopting subsequent decisions on the profile generated as part of the bad debt reports regarding the Data Subject held by the Central Risk Register and credit information systems. 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. The credit information systems are the banks' private databases consulted by banks and financial institutions to make credit assessments and to see information on payment punctuality and are required to assess the appropriateness of granting consumer credit, loans and financing in whatever technical form. The use of the Central Risk Register and credit information systems mean that customers with a good credit history can obtain financing more easily and under better terms and conditions. Banks and financial institutions use them to assess a customer's ability to repay financing granted. Therefore, the credit scoring system used in the credit application process, and the bad debt reports

regarding Data Subjects held by the Central Risk Register and credit information systems, may have the effect of preventing a Data Subject from being granted financing. The statistical analysis models or factors, and the decision calculation algorithm, indicators or points used as part of this process, are checked at least annually and are updated where the results of these checks require it.

6. Transfer of 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 the data

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

- entities which carry out banking, financial and insurance services;
- joint guarantors, guarantors and third-party payers;
- Regulatory Authorities and control bodies and, in general, public entities or private entities performing a public role (e.g. the Financial Intelligence Unit, the Bank of Italy, 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 apply);
- Public Bodies (economic and territorial) and Public Administration;
- trade associations;
- other companies of the Group to which the Bank belongs, or parent, subsidiary or associated company of any kind, in accordance with Article 2359, Italian Civil Code (even if these are located abroad);
- 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 in compliance with appropriate verification 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 and telecommunications network management services for the Data Controller (including mailing services);
- entities which print, envelope, transmit, transport and sort correspondence;
- entities responsible for document storage and data-entry;
- entities responsible for providing customer service activities to the Data Subject;
- companies managing national and international systems combating fraud against banks and financial intermediaries;
- professional firms or companies providing assistance and consultancy services (e.g. accountancy firms, law firms, etc.);
- companies that perform credit assessment, credit risk and insolvency identification, overindebtedness prevention and credit protection activities, including credit information systems;
- financial agents, credit brokers and other intermediaries operating in the credit, financial or banking sector, with the role of promoting and placing the Bank's products and/or services;
- entities providing the Interbank Corporate Banking (CBI) service;
- entities carrying out international financial operations (e.g. the "Society for Worldwide Interbank Financial Telecommunication" - SWIFT);
- 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 Bank, telemarketing etc.);
- entities responsible for controlling, auditing and certifying the Bank's activities;
- entities which, for various reason, succeed the Bank as owner of legal relationships (e.g. assignees or potential assignees of assets, credits and/or contracts).

The entities listed above work independently as separate Data Controllers, or as Data Processors appointed for this purpose by the Bank. A list of these entities, which is constantly updated, is available on the Bank's website www.bancaifis.it.

As part of the performance of assigned duties, Data may become known to the Data Controller's personnel, including interns, temporary workers, consultants, all specifically authorised to process personal Data.

In any case, personal Data will not be publicly disclosed and, therefore, will not be made available to unauthorised entities/individuals, in any form.

8. Storing and deletion of personal Data

In accordance with Article 5, paragraph 1, letter e) of the Regulation, Data will be held in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal Data were collected and processed, in compliance 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 law which governs storage 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 the storage times for marketing and profiling purposes). When this deadline expires, the Data will be deleted or anonymised, except where it must be held to comply with legal obligations or to fulfil orders given by Public Authorities and/or Regulatory Bodies.

9. The 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 that personal Data; b) rectification of inaccurate personal Data and to have incomplete personal Data completed; c) the erasure of personal Data which concerns them, where permitted by the Regulations; 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 concerning him or her, which he or she has provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those Data to another Data Controller, at any time, even where the relationship established with the Data Controller has ceased.

The Data Subject also has the right to object, at any time, to the processing of personal Data concerning him or her: in this case, the Data Controller is obliged to no longer process these data, save for the purposes allowed by the Regulation.

The Data Subject also has 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 him or her, unless this decision is: a) necessary for entering to or performing a contract between the Data Subject and a Data Controller; b) authorised by 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, the Data Subject has the right to obtain human intervention form the Data Controller, to express his or her 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.

A Data Subject also has 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 Banca Ifis 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 WITH REGARD TO FUND TRANSFERS USING THE SWIFT SERVICE

To carry out international financial transactions (e.g. a cross-border bank transfer) and some specific national transactions requested by customers, it is necessary to use an international messaging service. This service is managed by the "Society for Worldwide Interbank Financial Telecommunication" (SWIFT), with headquarters in Belgium.

The Bank communicates data to SWIFT (owner of the SwiftNet Fin system) regarding anyone who carries out these types of transaction (e.g. payer's name, payee's name, the name of their respective banks, bank details and the amount). Otherwise, the Bank could not carry out the transactions requested by customers.

It should also be noted that:

- all customer data used to carry out these financial transactions are – for reasons of operational security – currently duplicated and transmitted, and a copy is temporarily stored by SWIFT on one of the company's servers located in the United States;
- the data stored on this server is accessible and can be used in the USA, in accordance with local counter-terrorism legislation, by the relevant US authorities (e.g. the Department of the Treasury).

Data Subjects reserve all rights set out in legislation of the protection of personal Data.

PRIVACY POLICY WITH REGARD TO THE RECORDING OF TELEPHONE CALLS

The Bank wishes to inform Data Subjects who have an existing finance lease contract that it uses a system to record telephone calls as part of its activities to sell insurance by telephone in connection with leasing products already granted. These activities are carried out by a third-party company, specially designated as Data Processor. This recording system is aimed at providing proof of the foundation of relationships, managing the relationships and monitoring the quality of the service made available to the user. These recordings will be kept confidential and stored in accordance with the law at the third-party company's offices for 10 years from the moment in which their effects expire.

Telephone calls are recorded using automated systems which record outgoing calls. Appropriate measures are adopted that guarantee the security and confidentiality of the collected data, as set out by current legislation on the protection of personal Data. The audio files that are generated can only be accessed by individuals who are expressly authorised to process Personal Data.

The Bank wishes to inform Data Subjects who own an account contract that it uses a system to record inbound and outbound telephone calls managed by Customer Services in order to analyse and monitor the quality of the processes and services provided to customers, and to be used as proof in cases of any eventual disputes.

Telephone calls are recorded using automated systems which record incoming and outgoing calls. Appropriate measures are adopted that guarantee the security and confidentiality of the collected data, as set out by current legislation on the protection of personal Data. Recordings will be stored with restricted access and kept only for the time strictly necessary to achieve the purposes for which they were made. In any case, the maximum storage period will not exceed 10 years from the date the recordings were made, unless circumstances occur which require files to be stored for a longer period, in accordance with current legislation. Telephone call recordings can be accessed by persons expressly authorised to process personal Data, in order to protect the Bank's workers and company assets from direct or indirect damage which may result from disputes raised by customers, to monitor the quality of the service made available to the user, to fulfil internal audit obligations as set out by legislation and/or regulatory provisions to guarantee that customers and/or company assets are protected and to satisfy requests from external control bodies (Consob, Bank of Italy, external auditor, etc.), that are legally allowed to access telephone call recordings in their role as independent Data Controllers.

PRIVACY POLICY RELATING TO THE USE OF MOBILE APPLICATIONS

The Bank would like to provide this information to Data Subjects who have an existing current account and who use the "Banca Ifis Retail" mobile app, available to download from various app stores regarding the processing of personal Data that exists in the application. The "Banca Ifis Retail" app is developed, updated and maintained by CEDACRI S.p.A., and is legally owned by Banca Ifis S.p.A.

Personal Data are processed by the Data Controller to allow the Data Subject to use all the app's functionality and to ensure that it works correctly. For this purpose, the Bank uses technical cookies in its "Banca Ifis Retail" app. A constantly updated list of these cookies is available on the product's website. The user may also allow the app to integrate with the address list on the smartphone to share money, and to begin calls to contacts.

Personal Data processed in this way are protected by appropriate security measures which stop the "Banca Ifis Retail" app from working on devices on which it is installed that have been tampered with through the use of rooting/jailbreaking procedures.

The Data Subject may, at any time, have the Bank cease processing as described here by removing the "Banca Ifis Retail" app from their device.

INFORMATION IN ACCORDANCE WITH ARTICLE 6 OF THE CODE OF CONDUCT FOR INFORMATION SYSTEMS MANAGED BY PRIVATE PARTIES REGARDING CONSUMER CREDIT, RELIABILITY, AND PUNCTUALITY OF PAYMENTS

How we use your data

This policy pursuant to Art. 13 and 14 of Regulation (EU) 2016/679 is also provided on behalf of the credit information systems.

Dear Customer,

As the Data Controller, Banca Ifis S.p.A. would like to inform you that, in order to fulfil your request, it uses some of your personal data. This is information that you provide us or that we obtain by consulting certain databases.

These databases ("Credit Information Systems") containing information regarding the data subjects are consulted to evaluate, assume, or manage credit risk and to assess the data subject's payment punctuality and reliability. These databases are managed by private entities and used and supplemented by private entities belonging to the categories that you will find in the notice provided by the credit information systems managers.

We will keep this information in our records. Some of the information you provide, along with information related to your payment history related to the relationship that will be established, may be periodically communicated to the credit information systems.

This means that subjects belonging to the categories mentioned above, with whom you will request to establish a relationship, may know if you presented us with a request and if your payments are made regularly.

Processing and communicating your data is a requirement for finalising the contract. Without these data, we may not be able to fulfil your request.

The databases store this information based on the legitimate interests of the data controller to check the credit information systems.

Processing performed by the Bank

Your data may be transferred to a third country outside the EU or to an international organisation, in the manner provided for in paragraph 6 above.

According to the terms, methods and applicability limits established by current legislation, you have the right to check your data and exercise the various rights relating to their use (rectification, updating, erasure, limiting processing, opposition, etc.).
You may file a complaint with Garante [Italian Data Protection Authority] (www.garanteprivacy.it), as well as use the other means of protection provided by the applicable legislation.
We keep your data on file with us for the time required to manage your contractual relationship and to fulfil legal obligations (e.g., the provisions of Article 2220 of the Italian Civil Code on retaining accounting records).
Any request regarding your data may be sent to the Bank at privacy@bancaifis.it and/or the companies indicated below, to which we will communicate your data.
Your data may be used in the automated decision-making process for a request if this decision is necessary for the finalisation or execution of your contract with us. In particular, information obtained by consulting private databases relating to loans requested and provided by other financial intermediaries is processed by our systems in order to assess the financing request submitted to the Bank. If there is negative information found in the private database, the financing request made to the Bank is rejected, and this rejection is promptly communicated to the data subject.
We would also like to inform you that you can contact our Data Protection Officer, for any reason, at the following address: rpd@bancaifis.it.

Processing performed by the manager of the credit information systems

In order to better assess the credit risk, as well as the reliability and punctuality of payments, we communicate certain data (personal details, including those of the co-obligor, type of contract, amount of credit, and repayment methods) to the Credit Information Systems, which are governed by the relevant Code of Conduct and are independent data controllers. The data are also made accessible to the various private entities belonging to the categories that you will find in the information provided by the credit information system managers, available through the channels listed below.
Your data are periodically updated with information acquired over the course of the relationship (payment performance, residual debt exposure, the status of the relationship).
Within the credit information systems, your data will be processed according to the organisation, comparison, and processing methods strictly necessary for the purposes described above.
Your data are subject to statistical processing in order to assign you a summary judgement or score on your degree of reliability and solvency (credit scoring), taking into account the following main types of factors: including but not limited to the number and characteristics of existing credit relationships, payment performance and history in relation to existing or previous relationships, possible presence and characteristics of new credit requests, history of previous credit relationships, existence or non-existence of detrimental data, etc., which make it possible to obtain, through the application of statistical methods and models, results expressed in the form of summary judgements, numerical indicators or scores aimed at providing a predictive or probabilistic representation of the risk profile, reliability or punctuality of the payments of the data subject.
Some additional information may be provided if your credit request is not accepted.
The credit information systems we use are operated by:

1. IDENTIFYING INFORMATION: **ASSOCIAZIONE ITALIANA LEASING – ASSILEA**

CONTACT DATA: registered office in Via Massimo d'Azeglio no. 33, 00184 Rome (tel. +39 06/9970361 – Fax +39 06/45440739); website www.assilea.it;
MANAGER RESPONSIBLE FOR RESPONDING TO DATA SUBJECTS: ASSILEA SERVIZI S.r.l. (email: bdcr@assilea.it)
TYPE OF SYSTEM: positive and negative
DATA STORAGE TIME LIMITS: indicated in the table below
USE OF AUTOMATED CREDIT SCORING SYSTEMS: yes
EXISTENCE OF AN AUTOMATED DECISION-MAKING PROCESS: no

2. IDENTIFYING INFORMATION: **CRIF S.p.A.**

CONTACT DATA: registered office in Via M. Fantin, no. 1-3, 40131 Bologna (tel. +39 051/4176111 – fax +39 051/4176110); website www.crif.com; Data Protection Officer: dirprivacy@crif.com, crif@pec.crif.com.
TYPE OF SYSTEM: positive and negative
DATA STORAGE TIME LIMITS: indicated in the table below
USE OF AUTOMATED CREDIT SCORING SYSTEMS: yes
EXISTENCE OF AN AUTOMATED DECISION-MAKING PROCESS: no
OTHER: CRIF S.p.A. belongs to an international circuit of credit information systems operating in various countries inside and outside of Europe. Therefore, the information may be communicated to other companies (if provided for by law), even in other countries, that independently manage these credit information systems according to the laws in their countries, and process the information with the same purposes as the system managed by CRIF S.p.A.

3. IDENTIFYING INFORMATION: **Experian Italia S.p.A.**

CONTACT DATA: registered office in Piazza dell'Indipendenza no. 11/b, 00185 Rome; Consumer Protection Service: tel. +39 199183538 fax +39 199101850; Data Protection Officer: dpoItaly@experian.com; website: www.experian.it
TYPE OF SYSTEM: positive and negative
DATA STORAGE TIME LIMITS: indicated in the table below
USE OF AUTOMATED CREDIT SCORING SYSTEMS: yes
EXISTENCE OF AN AUTOMATED DECISION-MAKING PROCESS: no
OTHER: Experian Italia S.p.A., for purposes that are in any way related to assessing creditworthiness, making assessments on financial and cash flow situation and to prevent contrived or fraudulent acts, also processes data from public sources and is an indirect member of the Scipafi system. Data will be stored within the European Economic Area – EEA (the principal server is located in the United Kingdom). When they are subject to processing by entities outside the EEA, transfers are carried out to countries which have received a decision on suitability by the European Commission, that is, they are based on the Standard Data Protection Clauses adopted by the European Commission or on international programmes for the free circulation of Data (e.g. EU-US Privacy Shield Framework).
Further detailed information is available on www.experian.it (Consumer Area – Credit Information Systems Notice).
You have the right to access your data at any time. Contact our Bank, sending your requests to privacy@bancaifis.it or to the managers of the credit information systems at the addresses listed above.
In the same way, you may request the correction, updating or supplementation of inaccurate or incomplete data, or the erasure or blocking of Personal Data processed in violation of the law, or object to their use for legitimate reasons to be outlined in the request (Article 15 to 22 of Regulation (EU) 2016/679, excluding Art. 20).

Data storage time limits in the credit information systems:

financing request	no more than 180 days from the date of submission, if the request is accepted no more than 90 days from the date of the monthly update, if the request is not accepted or is subject to withdrawal
no more than two instalments or two months in arrears then rectified	up to 12 months from rectification
more than two instalments or two months in arrears then rectified	up to 24 months from rectification

delays or defaults that are not rectified	no more than 36 months from the relationship contract expiry date or from the date on which the most recent update was necessary and in any case no more than 60 months from the relationship contract expiry date
previous relationships in which all monetary obligations were paid	no more than 60 months from the termination of the relationship or the expiry of the related contract, or from the first update performed in the month following those dates over 60 months, when there are delays or defaults related to other credit relationships that are not rectified