

DATA PROTECTION NOTICE – Business to Business

Last updated **20th September 2023**

Introduction

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

BNP Paribas Real Estate and its affiliates are part of the BNP Paribas Group and offer a complete range of real estate-related services to its investors, developers, building occupants and public sector clients, at all stages of the real estate life cycle: real estate development, transaction, consulting, expertise, property management and investment management.

BNP Paribas Real Estate Advisory & Property Management UK Limited ("We"), as a controller, is responsible for collecting and processing your personal data in relation to our activities.

The BNP Paribas Group supports all its clients - individuals; entrepreneurs; small and medium-sized enterprises; large companies; multi-national groups and institutional investors - in their real estate, banking activities and in the realization of their projects, by providing appropriate financing, investment, savings and insurance solutions.

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

The purpose of this Data Protection Notice is to explain to you how we process your personal data, how you can control and manage it.

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

1 ARE YOU SUBJECT TO THIS NOTICE?

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

- one of our clients or in a contractual relationship with us (e.g., as a guarantor);
- a member of our client's family. Indeed, our clients 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 (including face to face, by phone, on our websites and applications, during events) so that we can contact you;

When you provide us with third party personal data, please ensure you inform such third parties about the disclosure of their personal data and invite them to read this Data Protection Notice. We will use our reasonable endeavours to do the same when possible (e.g., when we have the person's contact details).

2 HOW CAN YOU CONTROL WHAT WE DO WITH YOUR PERSONAL DATA?

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

If you wish to exercise the rights listed below, please submit a request by: (i) mailing a letter to the following address 5 Aldermanbury Square, London, EC2V 7BP; or (ii) contacting us via our email address REUK.GDPRBAU@realestate.bnpparibas with evidence of your identity (e.g. a scan/copy of your passport or driving licence) where required.

If you have any questions relating to our use of your personal data under this Data Protection Notice, please contact our Data Protection Officer via (i) a letter to the following address 10 Harewood Avenue, London, NW1 6AA, or (ii) via the Data Protection Officer email address data.protection@uk.bnpparibas.com

2.1 You can request access to your personal data

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

Your right of access to your personal data may, in some cases, be limited by applicable law and/or regulation. For example regulations relating to anti-money laundering and countering the financing of terrorism prohibits us from giving you direct access to your personal data processed for this purpose. In this case, you must exercise your right of access with the Information Commissioner's Office, which may request the data from us.

2.2 You can ask for the correction of your personal data

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

2.3 You can request the deletion of your personal data

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

2.4 You can object to the processing of your personal data based on legitimate interest

If you do not agree with a processing activity based on a legitimate interest, you can object to it, on grounds relating to your particular situation, by informing us precisely of the processing activity involved and the reasons for your objection. We will cease processing your personal data unless there are compelling legitimate grounds for doing so or it is necessary for the establishment, exercise or defence of legal claims.

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

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

2.6 You can suspend the use of your personal data

If you dispute the accuracy of the personal data we use or object to your data being processed, we will verify or review your request. During the period of studying your request, you have the possibility to ask us to suspend the use of your personal data.

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, including profiling, which produces legal effects concerning you or otherwise significantly affects you. However, we may automate such a decision if it is necessary for the entering into or performance of a contract between us, authorised by law or regulation or if you have given your explicit consent.

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

2.8 You can withdraw your consent

If you have given your consent to the processing of your personal data, you can withdraw this consent at any time.

2.9 You can request the portability of part of your personal data

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

2.10 How to file a complaint with the Information Commissioner

In addition to the rights mentioned above, you may lodge a complaint with the competent supervisory authority, which is most often that of your place of residence, as such, it is the Information Commissioner's Office in the United Kingdom.

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

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

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

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

3.1.1 We use your personal data to:

- monitor and report risks (financial, credit, legal, compliance or reputational risks etc.) that the BNP Paribas Group could incur in the context of its activities;
- assist the fight against tax fraud and fulfil tax control and notification obligations;
- record transactions for accounting purposes;
- prevent, detect and report risks related to Corporate Social Responsibility and sustainable development;
- detect and prevent bribery;
- detect and manage suspicious orders and transactions;
- comply with the provisions applicable to trusted service providers issuing electronic signature certificates;
- exchange and report different operations, transactions or orders or reply to an official request from duly authorized local or foreign financial, tax, administrative, criminal or judicial authorities, arbitrators or mediators, law enforcement, state agencies or public bodies.

3.1.2 We also process your personal data for anti-money laundering and countering of the financing of terrorism purposes

As part of a banking group, we must have a robust system of anti-money laundering and countering of terrorism financing (AML/TF) in each of our entities managed centrally, as well as a system for applying local, European and international sanctions.

In this context, we are joint controllers with BNP Paribas SA, the parent company of the Group (the term "we" in this section includes BNP Paribas Real Estate Advisory & Property Management UK Limited and BNP Paribas SA).

The processing activities performed to meet these legal obligations are detailed in Appendix 1 (Processing of personal data to combat money laundering and terrorist financing).

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

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

- evaluate whether 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;
- manage existing debts (identification of clients with unpaid debts);
- respond to your requests and assist you.

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

Where we base a processing activity on legitimate interest, we balance that interest against your interests 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 using the contact details provided in section 2 "HOW CAN YOU CONTROL WHAT WE DO WITH YOUR PERSONAL DATA" above.

3.3.1 In the course of our business activity of real estate, we use your personal data to:

- manage the risks to which we are exposed:
 - we keep evidence of operations or transactions, including in electronic evidence;
 - we monitor your transactions to manage, prevent and detect fraud;
 - we carry out the collection of debts;
 - we manage legal claims and defence our position in the event of litigation;
 - we develop individual statistical models in order to help define your creditworthiness.
- enhance cyber security, and manage our platforms and websites.
- use video surveillance to prevent personal injury and damage to people and property.

- enhance the automation and efficiency of our operational processes and client services (e.g., automatic filling of complaints, tracking of your requests and improvement of your satisfaction based on personal data collected during our interactions with you such as e-mails or chats).
- conduct statistical studies and develop predictive and descriptive models for:
 - commercial purposes: to identify the products and services that could best meet your needs, to create new offers or identify new trends among our clients, to develop our commercial policy taking into account our clients' preferences;
 - safety purposes: to prevent potential incidents and enhance safety management;
 - compliance purposes (e.g., anti-money laundering and countering the financing of terrorism) and risk management;
- organising promotional operations, conduct opinion and client satisfaction surveys.

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

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

Unless you object, we may send you these offers by electronic means, by phone or by post, for the products and services of the BNP Paribas Real Estate Group and those of the BNP Paribas Group and our trusted 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 client 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 your 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 as is visible in your client area);
- from your use of our various channels: websites and applications (e.g., if you are digitally aware, if you prefer a client journey to subscribe to a product, or service with more autonomy (self-care));

Unless you object, we will perform this customization based on standard profiling. If you consent, we may go further to better meet your specific needs by offering you products and services tailored to you.

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 withhold your consent or, if given, withdraw your consent at any time.

In particular, we ask for your consent for:

- tailor-made customization of our offers and products or services based on more sophisticated profiling to anticipate your needs and behaviours;
- personalization of our offers, products and services based on data about you;
- use of your navigation data (cookies) for commercial purposes or to enhance the knowledge of your profile.

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

4 WHAT TYPES OF PERSONAL DATA DO WE COLLECT?

We collect and use your personal data meaning any information that identifies or, together with other information, can be used to identify you.

Depending, among others, on the types of product or service we provide to you and the interactions we have with you, we collect various types of personal data about you, including:

- **identification information** (e.g. full name, identity, nationality, place and date of birth, gender, sex, identity card number, passport number, driver's license number, vehicle registration number, photo, signature);
- **contact information** private or professional (e.g. postal and e-mail address, phone number etc.);

- **property situation and family life** information (e.g. marital status, property ownership, number and age of children, study or employment of children, composition of the household, date of death of parents or spouse, property you own);
- **important moments in your life** (e.g. you have just married, divorced, lived as a couple, had children);
- **economic, financial and tax information** (e.g. tax ID, tax status, country of residence, income and others revenues, value of your assets);
- **education and employment information** (e.g. level of education, employment, employer's name, remuneration);
- **banking and financial information** (e.g. bank account details, products and services owned and used (credit, insurance, savings and investments), credit card number, money transfers, assets, declared investor profile, credit history, any defaults in making payments);
- **transaction data** (including full beneficiary names, address and transaction details including communications on bank transfers of the underlying transaction);
- **data relating to your preferences** (data which relates to your use of our products and services);
- **data from your interactions with us:** your comments, suggestions, needs collected during our exchanges with you in person and online during telephone communications (conversation), discussion by email, chat, chatbot, exchange on our pages on social networks and your complaints. Your login and tracking data such as cookies and trackers for non-advertising or analytical purposes on our websites, online services, applications, social media pages;
- **video protection** (including CCTV);
- **information about your device** (including technical specifications and uniquely identifying data); and
- **log-in credentials used to connect to BNP Paribas' website and apps.**

We may collect sensitive data such as health data, biometric data, or data relating to criminal offences, subject to compliance with the strict conditions set out in data protection regulations.

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., Companies House, the Financial Conduct Authority);
- 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 Group entities;
- from our clients (companies or individuals);
- from our business partners;
- 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?

6.1 With BNP Paribas Group's entities

As a member of the BNP Paribas Group, we work closely with the group's other companies worldwide. Your personal data may therefore be shared between Group entities, where necessary, to:

- comply with our various legal and regulatory obligations described above;
- fulfil our 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 of the Group's products and services that best meet your needs and wishes;
 - customise the content and prices of products and services.

6.2 With recipients outside the BNP Paribas Group and processors

In order to fulfil some of the purposes described in this Data Protection 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);
- 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 transactions (e.g., banks, correspondent banks, depositories, custodians, issuers of securities, paying agents, exchange platforms, insurance companies, payment system operators, issuers or payment card intermediaries, mutual guarantee companies or financial guarantee institutions);
- 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 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 or third party payment providers (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, 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 Group or our insurers.

7 INTERNATIONAL TRANSFERS OF PERSONAL DATA

In case of international transfers from the UK to a third country, the transfer of your personal data may take place on the basis of a decision by the UK Government where the UK Government has recognised that the country to which your data will be transferred ensures an adequate level of protection. In case of transfers of your personal data to a third country where the level of protection has not been recognized as adequate by the UK Government, 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 UK Government;

Binding corporate rules.

To obtain a copy of these safeguards or details on where they are available, you can send a written request to the address set out in section 2 above.

8 HOW LONG DO WE KEEP YOUR PERSONAL DATA?

For more information on retention periods, you can consult the Appendix 2 "Retention periods".

9 HOW TO CONTACT US

If you have any questions relating to our use of your personal data under this Data Protection Notice, or if you would like a copy of this Data Protection Notice in your native language, please contact our Data Protection Office using the details set out in section 2 above.

10 HOW TO FOLLOW THE EVOLUTION OF THIS DATA PROTECTION NOTICE

In a world where technologies are constantly evolving, we regularly review this Data Protection Notice and update it as required.

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

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

We are part of the BNP Paribas banking Group (“Group”) that must have a robust anti-money laundering and anti-terrorist financing (AML/CFT) system at entity level, centrally piloted, an anti-corruption mechanism, 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 we are established).

In this context, we act as joint controllers together with BNP Paribas SA, the parent company of the BNP Paribas Group (the terms “we” and “our” when used in this appendix therefore also cover BNP Paribas SA).

For the purposes of AML/CFT and compliance with International Sanctions, we implement the processing operations listed below to meet our legal obligations:

- A Know Your Customer (KYC) programme reasonably designed to identify, verify and update the identity of our clients, 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 we do 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:
 - o 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;
 - o involving directly or indirectly sanctioned territories, including Crimea/Sevastopol, Cuba, Iran, North Korea, or Syria;
 - o 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.
- Client 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 programme 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:

- o 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);
- o public information available in the press on facts related to money laundering, the financing of terrorism or corruption;
- o knowledge of a risky behaviour or situation (existence of a suspicious transaction report or equivalent) that can be identified at the Group level.

We may process special categories of data or criminal data since the purpose is to combat money laundering and terrorist financing.

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 is 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, 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]

Retention periods

Legal Basis	Macro-Purpose	Purposes	Retention Periods
		Manage risks (financial or legal, credit, compliance or reputational, etc.) that the BNP Paribas Group may face	Up to Six years but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Managing risks related to Corporate Social Responsibility and sustainable development	Up to six years but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
	Comply with market financial instrument regulations	Record communications, in accordance with the Markets in Financial Instruments Regulations (MIFID 2)	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Assess whether the provision of investment services is appropriate and appropriate to each client's profile, in accordance with market in financial instruments regulations (MIFID 2)	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
	Comply with legal obligations regarding financial security and professional ethics	Fight against tax fraud and meet our tax notification and control obligations;	Five years (from the date of an occasional transaction or the end of the relationship/contract), but, subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Participate in the prevention of corruption	Five years (from the date of an occasional transaction or the end of the relationship/contract), but, subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Combating money laundering and terrorist financing	Five years (from the date of an occasional transaction or the end of the relationship/contract), but, subject to business case, and/or legal, or regulation requirement, retention period can be longer.
	Comply with accounting and tax standards	Ensure the keeping of our accounts (see on other NPDs if there are other formulations)	Five years (from the date of an occasional transaction or the end of the relationship/contract), but, subject to business case, and/or legal, or regulation

			requirement, retention period can be longer.
		Fulfill our accounting and tax reporting obligations to the authorities	Five years (from the date of an occasional transaction or the end of the relationship/contract), but, subject to business case, and/or legal, or regulation requirement, retention period can be longer.

Legal Basis	Macro-Purpose	Purposes	Retention Periods
Respond to our legitimate interest or that of a third party	Manage litigation and pre-litigation	Retain proof of transactions	Limitation period, and subject to legal and regulation requirements of the transaction or contract
		Collect debts	Limitation period, and subject to legal and regulation requirements of the transaction or contract
		Handle legal claims and defences in the event of a dispute	Limitation period, and subject to legal and regulation requirements of the transaction or contract
	Keeping our clients, employees and operations safe	Improve cybersecurity, manage our platforms and websites, and ensure business continuity	Six years, (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Prevent bodily injury and damage to people and property via video surveillance	Six years but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
	Improve the efficiency of our processes and services	Automate our operational processes (e.g. automatic filling of complaints, follow-up of your requests)	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Optimize our client services (e.g. improving your satisfaction based on data collected during our interactions with you such as phone records, emails or chats)	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement,

			retention period can be longer.
Conduct statistical studies and develop predictive and descriptive models		For Commercial purposes: to identify the products and services we could offer you to best meet your needs, to create new offers or identify new trends among our clients and develop our commercial policy taking into account the preferences of our clients	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer
		For security purposes: to prevent potential incidents and improve security management (Health & Safety-Check)	Six years from the date of an incident but subject to business case, and/or legal, or regulation requirement, retention period can be longer
		For compliance purposes: fight against money laundering and terrorist financing and manage our risks	Five years (from the date of an occasional transaction or the end of the relationship/contract), but, subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		To fight fraud	Five years (from the date of an occasional transaction or the end of the relationship/contract), but, subject to business case, and/or legal, or regulation requirement, retention period can be longer.
Commercial prospecting		To offer electronically our products and services and those of other Group entities	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Offer by phone or paper mail our products, those of other Group entities or external partners	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Personalize our offers and services	Six years (from the date of an occasional transaction or the end of the

			relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Organize competitions, sweepstakes, promotional operations, conduct opinion and client satisfaction surveys	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.

Legal Basis	Macro-Purpose	Purposes	Retention Period
Performance of a contract or pre-contractual measures	Provide services or products and ensure client relationship management	Pre-assess the credit risk score and the repayment capacity of clients in conducting assessments on 1) loan-to-value; 2) affordability and 3) suitability for applicable products and services	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Provide and improve the products and services subscribed to in accordance with the contract	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Respond to your requests and assist you in your efforts	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.
		Manage payment defaults (e.g. identify clients in a situation of non-payment)	Six years (from the date of an occasional transaction or the end of the relationship/contract), but subject to business case, and/or legal, or regulation requirement, retention period can be longer.

Retention periods are established in accordance with the durations defined by the local regulations and contractual terms, and in compliance with local laws

All electronic records are subject to regular and routine backup with off-site storage.