DATA PROTECTION AND PRIVACY POLICY

May 2024

ATLANTICO EUROPA

INDEX

1. Introduction

The services provided by ATLANTICO Europa observe the highest quality standards and these are also the standards we use when processing the personal data we collect. With this in mind, this Data Protection and Privacy Policy (hereinafter "Policy") was prepared in accordance with the national and European legislation in force on the protection of individuals, more precisely in accordance with Regulation (EU) 2016/679 of the European Parliament and the Council, of 27 April 2016 ("GDPR"), as well as other legal and regulatory provisions and best practices.

The Policy describes the methods used by Banco Atlântico Europa SA. (hereinafter "ATLANTICO Europa" or the "Bank") to collect, process and use the personal data of its customers, potential customers or individuals having any other dealings with the Bank, or users of our website or mobile app (customer), as well as their rights in terms of this processing and how to exercise them.

Our internal security and privacy standards provide for:

- Processing the data fairly and lawfully;
- Not using the data collected for any purpose other than the collection purpose;
- Having security systems that prevent personal data from being accessed, changed or destroyed;
- Respect for the confidentiality of the data processed, especially from the employees of the data controller, with regard to the data they have access to under the scope of operations on the computer database, having been duly informed of the importance of compliance with this legal duty of secrecy and being responsible for compliance with this obligation of confidentiality.

2. Data controller

Banco Atlântico Europa SA is the controller of the personal data collected.

ATLANTICO Europa has a data protection officer who ensures that the Bank processes your personal data in compliance with the GDPR and that your rights as the subject of the data collected are complied with. If you wish to contact the Bank's Data Protection Officer, you can do so by sending an e-mail to dpo@atlantico.eu.

ATLANTICO Europa has a branch in Namibia, which is the Data Controller for the personal data of its customers, potential customers or individuals having any other dealings

with the branch, or users of our website or mobile app (customer), having appointed Banco Atlântico Europa SA. as its representative in the European Union. You can access the Data Protection and Privacy Policy of the Namibia branch of ATLANTICO Europa at www.atlantico.na.

3. The data we collect

Personal Data Category

ATLANTICO Europa collects the legally required data, as well as other data arising from the relationship between the Customer or potential Customer and the Bank.

To this end, ATLANTICO Europa may have access to the personal data of Customers and non-Customers, particularly identification or financial data, contacts, profession, nationality, schooling, social status, details on payment to and from their accounts, complaints, insurance taken out, details of contracts for services and products provided by ATLANTICO Europa, data on location, behaviour, communications (e-mails, letters, phone calls), specific device data, such as the hardware model and operating system version, exclusive identifiers of products and information on the mobile network used, type of browser, browser language, fingerprint/facial recognition, access to the internal and/or external memory, electronic signature, social relationships, public data, identification documents or copies of identification documents requested.

Special category data

Under the terms of the applicable law on personal data protection, some data are deemed to fall into a special category. Therefore, we only process these data with your consent or when there is a legitimate reason for this, expressly provided for by law.

The following data are deemed to be special category data: on racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, genetic data, biometric data, data on people's health, sex life or sexual orientation.

ATLANTICO Europa also stores the consents and proof of these, which includes information on how the Customer wants to be contacted and receive communications.

4. How we use your data

Legitimacy for personal data processing

In accordance with the data protection legislation, ATLANTICO Europa can only use the personal data collected when it has legitimacy for this, including transferring data to third

parties.

ATLANTICO Europa uses and transfers the personal data collected in the following situations:

- Execution of a contract with the Customer;
- Compliance with legal obligations;
- When it is in the legitimate interest of ATLANTICO Europa; or
- When the personal data holders consents.

There is deemed to be a legitimate interest whenever the Bank has a commercial or institutional reason to use the information, except when the fundamental interests, rights or freedoms of the subject prevail, requiring personal data to be protected.

Data transfer

The personal data collected by ATLANTICO Europa may be transferred to and processed by:

- Any organisation, agents, auditors, regulators, attorneys, public, government or police authorities or any individual or company when ATLANTICO Europa deems this is necessary for the processing purposes described above;
- Service providers, suppliers and consultants;
- Financial institutions and payment service providers;
- Authorities or other official bodies located in the European Union or abroad, in order to aid in the prevention of terrorism, money laundering and other crimes;
- Under the scope of transactions or other services involving the disclosure of personal data on behalf of a Customer or a counterparty;
- Under the scope of banking operations, personal data may be processed and disclosed as described above in any country where ATLANTICO Europa does business or has a service provider, as long as an adequate level of protection is assured.

Communications and commercial information

The data collected may also be used by ATLANTICO Europa for marketing purposes and the communication of campaigns, products and services deemed to be of interest to the

Customer, particularly by sending e-mails and text messages, making phone calls and by other electronic means.

During the execution of the Contract and while there is a relationship with the Customer, ATLANTICO Europa may identify banking and financial products and/or services that may be of interest to the Customer. In this context, ATLANTICO Europa may use the definition of Customer profiles/segmentation and other data processing techniques with the aim of carrying out commercialisation and direct marketing campaigns, after client approval.

When collecting and processing the data of non-Customers, ATLANTICO Europa will always request express, free and informed consent when it is a question of processing the data for any one of the purposes indicated above, particularly for marketing purposes and the communication of campaigns, events, products and services.

If any Customer or non-Customer does not wish to receive these communications, they may inform ATLANTICO Europa of this by exercising their right to object to the processing of data for this purpose.

Automated processing

ATLANTICO Europa uses automated processing of all the personal data provided and obtained, directly or indirectly, as a result of operations carried out for the purpose of managing the relationship with Customers and non-Customers.

The Bank uses the information collected for decision-making, based on the automated processing and definition of profiles, for opening accounts, adapting products and services in order to include the Customer in Customer segments, to present products and services based on the different Customer segments, fraud detection and credit approval.

Data subjects are entitled not to be subject to any decisions made exclusively based on automated processing, including the definition of profiles.

5. Storage period

ATLANTICO Europa stores your personal data for as long as:

- you are a Customer;
- the reason for processing the data collected still holds;
- justified for legal or regulatory reasons.

Personal data will be stored in accordance with the principles of privacy and protection of private life. The data collected are used only for the purposes indicated below.

List of the purposes for which we can use the personal data of our customers, potential customers or individuals having any other dealings with the Bank, as well as an indication of the legal basis for the data processing carried out by ATLANTICO Europa and the data storage periods:

PURPOSES OF PROCESSING	LEGITIMACY	DATA STORAGE PERIOD
• Management of the Bank relationship with customers or their businesses (i.e. keeping up-to-date customer records, contact management, replying to requests for clarification). • Account opening and management • Subscribing to and management of financial products and services. • Loan granting and management • Assignment of credits (i.e. credit securitisation operations) • Managing banking operations • Complaints management • Testing/subscribing to new products for a period of time	Contractual compliance	During the contractual relationship, except when it is necessary to keep their personal data for longer than the duration of the contract, based on legitimate interests or when legal obligations so require.
• Development of marketing activities • Studying how Bank customers use products and services provided by the Bank or other organisations (to define customer types and for the	Consent	Until consent is withdrawn

Bank to be more efficient in the way it complies with its legal and contractual obligations). • Use of cookies for re-marketing		
Monitoring service quality through call recording	Consent	30 days since its collection
Proof of signing a contract or the interest shown in a future contractual relationship through call recording	Consent	7 years from the operations in question
Managing security and crime prevention - Prevention of Fraud/Money Laundering (use of personal data to check if customers' personal accounts are being used for fraud or money laundering. If there is any risk of fraud, the Bank may suspend activity in the Customer accounts or refuse access).	Compliance with legal or regulatory obligations	7 years
• Risk management (i.e. credit risk management) • Communications with public authorities, particularly regulatory bodies (e.g. the CMVM Securities and Exchange Commission, Banco de Portugal, the Tax Authority, the Foreign Account Tax Compliance Act, 2010 (FATCA), the Credit Risk System, the European Central Bank)	Compliance with legal or regulatory obligations	During the pre-contractual and contractual phase with the customer, except when it is necessary to keep their personal data for longer than the contract duration, based on legitimate interests or when legal obligations so require.
Video surveillance	Legitimate interest	30 days

• Service satisfaction and quality assessment (satisfaction surveys) • Development of products and services	Legitimate interest	During the pre-contractual and contractual phase with the customer
Monitoring entries via reception	Legitimate interest	180 days
Internal and external audits (i.e. audits for certificate issue)	Legitimate interest	During the pre-contractual and contractual phase with the customer, except when it is necessary to keep their personal data for longer than the contract duration, based on legitimate interests or when legal obligations so require.

6. Sending data to a third country

ATLANTICO Europa may send the data collected to third countries in the following circumstances:

- Management of the contractual relationship with the Customer;
- Compliance with legal duties;
- Relationship with consultants to help in the management of their accounts and services.

The transfer of information to third countries will be assured and processed the same way and with the same assurances, particularly the exercise and enjoyment of the rights assigned and the effective, corrective legal measures used in the processing of information collected and processed in the European Union.

7. Data processing security

One of the Bank's fundamental pillars is the guarantee of privacy and information security. Among the numerous measures already implemented in the Bank's systems and organization, physical, electronic, and procedural safeguards are in compliance with the applicable legal

standards for the protection of such information, against unauthorized access and use, alteration, and destruction.

Its employees are held accountable for compliance with the policies, procedures, rules and regulations on the privacy and confidentiality of information.

To this end, ATLANTICO Europa implements logical, physical, organisational and security measures that are adequate, necessary and sufficient for protecting the personal data of its Customers and non-Customers against destruction, loss, alteration, disclosure, unauthorised access or any other accidental or illegal forms of processing, in particular:

- Security requirements and measures, the use of firewalls and intrusion detection systems, the existence of a strict policy on access to systems and information and logging the actions taken by employees on the personal data of Customers or users;
- Physical security measures, with monitoring of access to the physical installations and image recording, pursuant to the law in force;
- Privacy by design;
- Use of technical methods such as encryption, scrambling, pseudonymisation and anonymisation of personal data;
- We follow the ISO 27001 security regulations, on the basis of which our information security policy was designed.
- If the Bank uses external providers (contracted agents, third companies or persons other than Bank staff) that need to access internal information, they are expected to maintain confidentiality and to adopt the security procedures identified by the Bank. Access to information by these parties will be restricted to the information necessary for them to do the work they were contracted for.

Notwithstanding the policies implemented by the Bank, Customers should keep their access codes secret, not sharing them with third parties, and adopt safe behaviour in relation to their equipment, thus ensuring their security.

8. Rights of Data Subjects

The Bank undertakes to assure the exercise of the following rights: access, rectification, restriction, erasure and portability.

- Right of access to the personal data processed and information on these. The right to see/hear or get a copy of documents such as contracts, written agreements or calls they are party to and that are recorded;
- Right to rectification of personal data which are inaccurate or asking for incomplete data to be completed;
- Right to erasure (or "right to be forgotten") of personal data, provided there are no valid or legal reasons requiring them to be kept;
- Right to object or withdrawal of consent at any time, such as in the event of data processing for marketing purposes, provided that no legitimate interests prevail over your interests and without compromising the lawfulness of the processing carried out based on the consent previously given;
- Right to restriction of processing, i.e. the right to request the restriction of the processing of your personal data, particularly through the inclusion of a mark on the personal data kept in order to restrict any future processing;
- Right to portability, i.e. the right to receive your personal data in a commonly used, machine-readable format or to request the transmission of these data to another controller;
- Right to complain to the Bank via registered letter and/or to a supervisory and control authority. In Portugal, you can lodge your complaint with the National Data Protection Commission.

To exercise their rights such as accessing their data, requesting its rectification, deletion, or opposition to its treatment in accordance with the law, customers must complete the "Exercise of Rights" form provided by ATLANTICO Europa and submit it to the designated addresses:

Banco ATLANTICO Europa
C/o: Data Protection Officer (DPO)
Avenida da Liberdade, nº 259
1250-143 Lisboa

ATLANTICO Europa has appointed a Data Protection Officer who is available to provide any clarification related to the processing of your personal data. For further information, please contact:

E-mail address of Data Protection Officer - dpo@atlantico.eu.

ATLANTICO Europa, aims to respond to all requests within 30 days, however, in the case of complex requests, may need to extend this timeframe by up to 60 days. If this is necessary, we will provide the reasons for the delay to the request holder.

9. Changes to the Privacy Policy

This Data Protection and Privacy Policy may be changed by ATLANTICO Europa, particularly for reasons of compliance with legal obligations. The data subjects will be informed of any such changes. All the changes made come into force when published, unless otherwise indicated.

10. Tips for safe use

- Update your computer regularly;
- Use only licensed software;
- Install an antivirus program, keep it up-to-date and perform regular analyses;
- Avoid using hardware (USBs, discs, CDs) from unknown sources, as they may contain viruses, malware or tools that allow access to your computer;
- Install and configure a personal firewall;
- Define strong passwords and change them regularly, making they more complex by mixing letters (capital and small), numbers and symbols. Don't use your name, family names or birthdates as passwords. Memorise them and never give them to other people.

Mobile devices:

- Define an access password for your device with automatic locking;
- Protect your device with an antivirus app and allow automatic updates;
- Disable the option to install apps from unknown sources, i.e. avoid apps that are not supplied by official stores;
- Before installing an app, confirm the features and permissions it asks you for (e.g. a flashlight app does not need access to your contacts, text messages or e-mails);
- Never click on links sent in text messages from unknown sources. Delete the message and block the sender. If it is from a reliable source, we suggest

confirming the accuracy of the content by contacting the source before accessing the link.

- Beware of text messages asking for a reply with personal data. They might not contain malicious software, but it could be a means of gathering contacts for spam campaigns;
- Be suspicious if you get lots of unsolicited e-mails or text messages. This could mean there is a malicious program on your mobile phone;
- Back up your information regularly so that you will have an up-to-date copy in the event of loss, theft or damage;
- Disable Bluetooth when you don't need it. The Bluetooth communication protocol has security bugs that can be used by third parties to hack your device. It also reduces battery consumption;
- If you send equipment for repair:
    - Remove temporary files and the cache stored in the memory of your equipment;
    - Clear your internet browser history;
    - Check the personal data you leave on the equipment.

<u>On the Internet:</u>

- Don't open e-mail messages from dubious sources;
- Don't run files or links obtained via e-mail, especially those from unknown sources;
- Check the security certificate for the websites you visit, ensuring it belongs to the site you want (address begins with https:// and has a padlock);
- In the case of ATLANTICO Europa, the certificate clearly identifies the name of the Bank;
- Always prefer accessing MYATLANTICO using the link on our page, avoiding links you may have received by e-mail;
- You can read our Cookies policy at: atlantico.eu or atlantico.na;
- Clear your browser history regularly.