DATA PROTECTION NOTICE

November 2025

1 INTRODUCTION

The protection of your personal data is of utmost importance to Advanzia Bank S.A. (*"the Bank"*), a financial institution based in Luxembourg, Trade Register under number B 109 476, operating the website https://www.advanziakonto.com/?lang=EN.

This notice applies to the Bank's customers, applicants, web users, legal representatives, heirs or other individuals contacting the Bank via e-mail or other communication channels (*"you"*). Please note that this notice applies in the context of the Bank's deposit accounts.

The Bank ensures the right to the protection of personal data for you, a fundamental right, as part of the Bank's social responsibility. The Bank's compliance with the transparency obligations set by the General Data Protection Regulation (*"GDPR"* or Regulation (EU) 2016/679) is key for this purpose. This Data Protection Notice ensures that the Bank's processing activities are transparent to you and that you are able to exercise your rights under GDPR.

Please be informed that this document is a general Data Protection Notice that gives an overview of processing personal data in relation to the service offered to you. However, the Bank applies a layered approach for data protection related notices and other processing activities may have a more specific Data Protection Notice.

2 WHAT DATA CATEGORIES ARE PROCESSED?

The Bank processes the following categories of your personal data:

a) Contact and identification data provided by you during your application: gender, title, first name, last name, mobile number, e-mail, country of residence, postal code, city, street name, house number, nationality, second nationality (optional), date of birth, city of birth, fiscal country residence, tax identification number (TIN), confirmation if you are not a US person.
b) Account information the Bank generates once your account is created: IBAN, account balance, interests.
c) Data the Bank creates to internally refer to you: Pega application number, customer ID, T24 account number.
d) Communication e.g., by phone, e-mail, letter, contact form.
e) Copy of documents: copy of identity document, copy of passport, residence permit, proof of residence, power of attorney, self-assessment form (including data categories specified in point a) above).
f) Data relating to your online behaviour and account, e.g. username, IP address, device ID, type of device or operating system used. Only aggregated data is created on web behaviour on the Bank's websites (indirect collection of data).
g) Data related to the KYC/AML checks (i.e., *"Know Your Customer"*, anti-money laundering), carried out by the Bank in accordance with the Luxembourg law of 12 November 2004 on the fight against money laundering and terrorist financing. This entails data received from third parties, publicly available data about you, potentially including your social media profiles (indirect processing of data).
h) Recording of phone calls with contact centre agents.
i) Video recording of the facial recording process revealing your identity document and facial image (biometric data).

Most of the above data categories are collected directly from you, except for example for KYC/AML checks or aggregated online behaviour.

With the exception of biometric data for identification purposes, the Bank does not ask you for any sensitive personal data, nor the Bank intends to process data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

3 WHY IS YOUR DATA PROCESSED?

3.1 Based on your consent

You may provide the Bank with your explicit consent for facial recognition before the video identification starts during your application on a specific page dedicated for this purpose (Article 9(2)(a) GDPR). Your explicit consent applies for training Namirial's AI model.

The following other purposes are based on your prior consent (Article 6(1)(a) GDPR):

- For marketing purposes, you can agree to be contacted by Advanzia Bank via phone, text message or email about interesting offers regarding the Bank's products as well as other financial services mediated by the Bank.
- The Bank records phone calls with contact centres, following a disclaimer provided at the beginning of the call.

3.2 To fulfil contractual obligations

Please note that most of the personal data listed in Section 2 are necessary for the Bank's contractual relationship with you and for providing services to you (Article 6(1)(b) GDPR). Therefore, if you decide not to provide your personal data, the Bank will not be able to proceed with the conclusion of your contract or provide you with the Bank's services. The following purposes are necessary to take precontractual steps or to fulfil contractual obligations:

- Onboarding process: the examination and acceptance of your respective application, reapplied process.
- Issuing a qualified electronic signature (*"QES"*).
- Processing of customer enquiries.
- Payment execution and handling.
- Customer request handling (emails, calls and follow-up) and contact centre management.
- Post handling and scanning of physical documents.
- Deceased customer handling (in the context of heirs and legal representatives).
- Maintaining the MyPage.
- Checking non-EU addresses.
- Internal legal processes such as contract review.
- Internal financial processes such as checking the nostro account, payment handling, partner invoicing.
- Provision of bank statements.
- The execution of the services the Bank provides to you.

3.3 To comply with legal obligations

The Bank is required to process your data for compliance with legal obligations under both EU law, the law of Luxembourg or the law applicable in the respective market (Article 6(1)(c) GDPR). With this in mind, the Bank has legal obligations to process your personal data within the following frameworks:

- Customer due diligence, identity and age verification.
- Anti-money laundering and counter-terrorist financing (*"AML/CTF"*).
- If you are not a resident in Luxembourg, the annual report to the tax authority of Luxembourg under the Directive on Administrative Cooperation (*"DAC"*) and Common Reporting Standard (*"CRS"*) frameworks (providing data categories a), b) and c) as per Section 2).
- Dormant account process.
- Risk management of the Bank.
- Cooperation with authorities such as CSSF, CNPD, law enforcement.
- Dispute handling, care cases (in the context of caretakers).
- Transaction monitoring, payment screening, high balance approvals.
- Operating the Bank's information security framework, e.g. access rights monitoring.
- Litigation case management, relation with judicial authorities.
- Financial processes such as securitisation.
- External or internal auditing which may reveal personal data.
- Handling of complaints, data breaches and data subject requests.

3.4 Based on the Bank's legitimate interests

The Bank may process your personal data based on the Bank's or third parties' legitimate interests (Article 6(1)(f) GDPR):

- Checking and improving data quality (e.g. checking with data from telephone directories).
- Testing and optimisation of processes for needs analysis in order to address customers directly.
- Marketing processes such as analysing web users, applicants and customers, AI landing page engine, co-registration partnerships and essential cookies.
- Assertion of claims/demands and defence in legal disputes.
- Ensuring the Bank's IT operations such as the internal Service Desk, application support, infrastructure on demand, development, UAT testing and incident management.
- Measures for the further development of services and products.
- Measures to assess risk factors for the Bank.
- Aggregated data analytics for internal reporting.
- Business and strategic review, mergers and acquisitions, setup of subsidiaries (if any).

4 WHO CAN ACCESS YOUR DATA?

To achieve the purposes described in this Data Protection Notice, the Bank may, share your personal data with:

Category	Company
Application processing	Pegasystems Inc. (data storage in EU with exceptional access from the US).
Address verification	IDCanopy Flexco (Austria)
Contact centres	Transcom Halle GmbH, M Plus Croatia d.o.o. (with centres in Croatia, Serbia, Bosnia and Herzegovina, Egypt)
IT services	Microsoft Azure (EU)
Payment system	Temenos (EU) for operating T24
Printing, scanning, archiving, billing, bank statements	Streff (Luxembourg), Imprimerie Centrale (Luxembourg)

Facial recognition and QES	Namirial SpA (Italy)
Authorities	CSSF, CNPD, Luxembourg tax authority (ACD), law enforcement authorities, financial intelligence unit, prosecutor's office for compliance with legal obligations and courts for litigations.
Nostro account	ING Belgium
External auditors and consulting	E.g. KPMG, PwC, Deloitte, EY (Luxembourg)

5 INTERNATIONAL DATA TRANSFERS

International data transfers mean transmitting personal data outside the EU/EEA (to so-called "third countries"). Where possible, the Bank aims to choose IT services that are based in the EU. However, due to technical constraints, some of these services are partly taking place in the US or UK. In those cases, the Bank primarily uses Standard Contractual Clauses of the European Commission accompanied by transfer impact assessments or the UK Addendum to safeguard your rights. Regarding commercial organisations based in the US, the Bank aims to conclude contracts with US companies that are active on the EU-US Data Privacy Framework's List when possible.

In addition, the Bank relies on Standard Contractual Clauses with regard to the Bank's contact centres that are located outside the EU (Serbia, Bosnia and Herzegovina) with transfer impact assessments in place.

6 HOW LONG DO THE BANK STORE YOUR DATA?

The Bank automatically deletes or anonymises your data after the following periods:

- **4 days** for video recordings during the biometric identification strictly for fraud prevention purposes.
- **90 days** for recorded phone calls.
- **90 days** for video recordings created during facial recognition for training Namirial's AI model. Consent can be withdrawn in this context.
- **2 years** for communication with third parties with no contractual or business relationship with the Bank.
- **5 years** after the application concerning both accepted and rejected applicants. This period is based on the Bank's legitimate interest in case of rejected applications. In principle, rejected applicants may exercise their right to erasure ("right to be forgotten") as explained below, unless the data is necessary for legal obligations, compelling legitimate interests or litigation.
- **5 years** for retaining images related to facial recognition on the Bank's side for compliance with AML/CTF obligations.
- **10 years** after the end of the business relationship or last transaction. If you are a customer, the Bank retains your personal data during the contractual relationship, which is necessary for the provision of the Bank's services to you. In addition, your personal data is retained for a period of 10 years after, as per the Bank's AML/CTF obligations.
- **20 years** after the application for the technical files related to QES for evidencing purposes, which is stored by Namirial as required by Italian law.
- Up to **30 years** in exceptional circumstances in case of civil litigation.

7 WHICH RIGHTS DO YOU HAVE?

7.1 Right of access

If you wish to have access to your personal data, the Bank will provide you with a copy of your personal data in accordance with your request.

7.2 Right to rectification

If you believe that your personal data is inaccurate or incomplete, you can ask the Bank to correct it. For simple updates of e.g. phone numbers or postal address, please refer to the web portal. For more complex requests, please note that the Bank may request supporting documentation to verify your data.

7.3 Right to erasure ("right to be forgotten")

If you wish, you can ask the Bank to delete your personal data, within the limits of the Bank's legal obligations. In general, you may request to delete your personal data if you are an applicant for the Bank's services. If you are a customer, please be aware of the data retention obligations specified in Section 6.

7.4 Right to restriction of the processing

You can also ask to restrict the processing of your personal data, in particular if you consider it inaccurate or object to the processing of your personal data. Please note that in that case the data in question will be restricted for the time it takes the Bank to investigate your request and the Bank may not be able to provide you with services in this period.

7.5 Right to data portability

You can request the Bank to receive your personal data in a structured, commonly used and machine-readable format. The Bank can also send it to third parties if you wish. However, please note that this right is limited to personal data where it is processed based on your contract and where the processing is carried out by automated means (i.e. not paper-based). In addition, this right is without prejudice to the Bank's obligation with regard to professional secrecy, as laid down in the Luxembourg Law on the Financial Sector of 5 April 1993.

7.6 Right to object

If you do not agree with a processing activity carried out based on legitimate interest (specified in Section 3.4), you may object to the processing of your personal data, for reasons specific to your circumstances, by precisely indicating which processing you are objecting to.

If you object to a processing activity, the Bank will stop processing your personal data related to that activity, unless there are compelling legitimate grounds for them, or if his is necessary in order to establish, exercise or defend legal claims.

7.7 Your rights related to automated decision-making (facial recognition)

Namirial's facial recognition is automated decision-making process based on artificial intelligence (AI) part of the Bank's onboarding process. Namirial compares your facial image with the photo on your identity card to verify your identity, to facilitate the conclusion of your contract with the Bank, and to issue a qualified electronic signature. You may be

automatically rejected due to technical issues, image quality issues or suspected fraud. Related to facial recognition, you have the right to:

- Ask for human intervention e.g. to ask the Bank for necessary assistance to finish your application,
- Express your point of view or contest the decision,
- Withdraw your consent,
- Request an alternative process without the use of AI or biometric data to respect your freely given consent.

7.8 Right to withdraw your consent

You can withdraw your consent at any time in relation to the processing activities based on your consent. In the context of facial recognition, it means that your images from Namirial will be deleted to prevent them for the use of training the AI model.

8 HOW CAN YOU CONTACT THE BANK?

Should you have any questions related to the protection of your personal data, or if you would like to exercise your rights under the GDPR, please contact the Bank at dataprotection-deposit@advanzia.com. The Bank is also at your disposal via post: Data Protection Officer, Advanzia Bank S.A., 14, Rue Gabriel Lippmann, L-5365 Munsbach.

9 WHERE CAN YOU LODGE A COMPLAINT?

Should you wish to lodge a complaint at the supervisory authority competent in Luxembourg, CNPD, you can do so at https://cnpd.public.lu/en/particuliers/faire-valoir.html.