DATA PROTECTION NOTICE

July 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.advanzia.com/en-gb/, and other B2B websites in cooperation with its partners.

This notice applies to the Bank's customers, applicants, web users, on-site visitors, legal representatives, heirs or other individuals who contact the Bank via email ("you"). Please note that this notice applies in the context of the Bank's credit card and deposit account services.

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. In addition, the purpose of this Data Protection Notice is to comply with the Act of 1 August 2018 of Luxembourg on the organisation of the National Data Protection Commission and on implementing 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 services offered in different countries in the EU. As the Bank applies a layered approach on public documents on personal data protection, other processing activities under the Bank's control or different markets have a more specific data protection notice.

2 WHAT DATA CATEGORIES ARE PROCESSED?

The Bank processes the following categories of personal data:

a) Contact and identification data: title, first name and surname as in the ID card, mobile phone number, e-mail address, country, address (postcode, city, street, number, optional: block, stairs, door), place of birth, nationality, date of birth.
b) Financial information at the time of application: net income (monthly or annual), credit card available, occupation, length of employment, marital status, type of residence, length of stay.
c) Copy of documents (upon request): an identity document, a passport, a residence permit, a salary certificate or a power of attorney.
d) Account information: IBAN number, card number, card information, PIN number, control number, security code, balances in your account, money orders, credit card transactions, fees, rewards, debit interest, late payment interest, and monthly outstanding amounts.
e) Communication, e.g. by telephone, e-mail, letter, contact form, information on the Bank's contractual relationship.
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) Information relating to your creditworthiness, such as Advanzia's internal credit score, external scores by agencies, debts and collections at other financial institutions, civil litigation related to indebtedness, etc. (indirect collection of data).
h) Data related to the KYC/AML checks (i.e., "Know Your Customer", anti-money laundering), conducted 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).
i) Recording of phone calls with contact centre agents.
j) 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, aggregated online behaviour, credit scoring and fraud prevention.

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

3 WHY IS YOUR DATA PROCESSED?

3.1 Based on your consent

Depending on the market, 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).

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

- You may consent to Advanzia Group (Advanzia Bank and Advanzia Insurance AB) for marketing purposes by ticking a checkbox on the Bank's website (opt-in). This appears when applying for the Bank's products, allowing to inform you in the future by telephone, SMS, or email about offers, as well as about other financial services. This includes for example campaigns related to card activation, usage, customer retention and churn prevention.
- The Bank records phone calls with contact centres, following a disclaimer provided at the beginning of the call.
- Optional cashback services, available through the Advanzia app in Germany and Luxembourg.
- Open banking (in Spain only).

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").
- Card embossing and delivery.
- Customer request handling (emails, calls and follow-up) and contact centre management.
- Post handling and scanning of physical documents.
- Payment execution and handling.
- Provision of bank statements and invoices.

- Assessment of your creditworthiness after the conclusion of your contract for the purpose of potentially increasing your credit limit.
- Collection, including internal reports (“collection splitter”), transfer to collection agencies, payments received during collection.
- Deceased customer handling (in the context of heirs and legal representatives).
- Maintaining the MyPage and Advanzia app.
- Checking non-EU addresses.
- Internal legal processes such as contract review.
- Internal financial processes such as checking the nostro account, payment handling, partner invoicing.
- Supporting your application process with the Bank’s B2B Partners and exchange on your credit card status (if you applied via a B2B partner).

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:

- Creditworthiness assessment before entering into a contract with the Bank.
- Customer due diligence, including identity and age verification.
- Anti-money laundering and counter-terrorist financing (“AML/CTF”).
- Application fraud prevention and transaction fraud monitoring.
- Obligations under tax law, such as CRS and FATCA reporting.
- Risk management of the Bank.
- Cooperation with authorities such as CSSF, CNPD, law enforcement.
- Dispute handling, chargeback, insolvencies, care cases (in the context of caretakers).
- Credit limit reassignment.
- 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, CESOP reporting.
- Account and card management, 3D Secure Authentication, authorisations for payments by TSYS, statement cycle processing.
- External or internal auditing which may reveal personal data.
- Handling of complaints, data breaches and data subject requests.

3.4 Based on legitimate interest

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

- Ongoing exchange with credit scoring agencies.
- Occasional analysis (“one-off tests”) of larger volumes of customer data provided by credit scoring agencies for the purpose of optimising the Bank’s model for creditworthiness assessment.
- Marketing processes such as analysing web users, applicants and customers, AI landing page engine, co-registration partnerships and essential cookies.
- Ensuring the Bank’s IT operations such as the internal Service Desk, application support, infrastructure on demand, development, UAT testing and incident management.
- Detecting and handling prohibited uses of cards during collection (“restart using cards”, “overlimit” processes).

- Trustpilot and Google Maps review management.
- Write-off management.
- Registration of on-site visitors, organisation of events, video surveillance.
- Management of internal media database of journalists, social media management (e.g. LinkedIn).
- Aggregated data analytics for internal reporting
- Non-performing loan management and portfolio optimisation.
- Anonymised data monetisation.
- Business and strategic review, mergers and acquisitions, setup of subsidiaries (if any).
- Improving fraud prevention by training AI models: in order to continuously improve the security of our services and detect fraud attempts more effectively, we process images of ID documents to train our AI models. This processing is used to detect forgery features and anomalies on the documents themselves. No biometric data generated during face matching is used for this purpose. This processing is based on the legitimate interest of the Bank and Namirial to prevent fraud and ensure the integrity of the identification process.

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
Advanzia App	Okta, Inc. (US-based with storage primarily in EU)
Anonymised data monetisation	Fable Data Limited (UK)
Application processing	Pegasystems Inc. (data storage in EU with exceptional access from the US).
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.
B2B partners (if applicable)	E.g. Hilton, Turkish Airlines, Intersport
Card embossing	Idemia (EU)
Cashback provider	Etvas GmbH (Germany)
Contact centres	Transcom Halle GmbH, M Plus Croatia d.o.o. (with centres in Croatia, Serbia, Bosnia and Herzegovina)
Co-registration partners (if applicable)	E.g. Financeads, Check24 GmbH, Sovendus GmbH, Userwerk, Salenti or Compare Verlag (Germany)
Credit scoring agencies	Germany: Boniversum GmbH, SCHUFA Holding AG, Experian GmbH Austria: KSV1870 Holding AG, CRIF GmbH Spain: Experian Bureu De Crédito S.A.U., ASNEF-Equifax Italy: Crif SpA, Experian SpA France: Banque de France
Debt collection agencies (EU)	Depends on the market and your specific situation.
Delivery services	DHL, Deutsche Post AG (EU)
External auditors and consulting	E.g. KPMG, PwC, Deloitte, EY (Luxembourg)
Facial recognition and QES	Namirial SpA (Italy)
Fraud prevention	LexisNexis (Ireland) (Emailage and ThreatMetrix services), Telesign (Belgium)
IT services	Microsoft Azure (EU)
Non-performing loans	Dignisia AB (Sweden)
Nostro account	ING Belgium
Payment and transaction systems	Mastercard, Visa (EU and US), TSYS (EU and US), Broadcom (US)
Printing, scanning, archiving, billing, bank statements	Streff (Luxembourg), Imprimerie Centrale (Luxembourg)

Subsidiary	Advanzia Insurance AB (Sweden), strictly in the context of marketing opt-in for insurance products.
Transaction monitoring	UAB AMLYZE (Lithuania)

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 IS YOUR DATA STORED?

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

- **90 days** for recorded phone calls.
- **90 days** for images of identity documents that may be processed on the basis of our legitimate interest to improve fraud prevention (training of the AI model).
- **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.
- **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 or Advanzia app. 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 if you 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 its services during 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 so. However, please note that this right is limited to personal data where it is processed based on your consent or 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

You may object to the processing of your personal data, in particular if you do not agree with a process carried out based on legitimate interest, for reasons specific to your specific 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 this is necessary in order to establish, exercise or defend legal claims.

7.7 Your rights related to automated decision-making

7.7.1 Credit scoring

The Bank relies on automated decision-making, including profiling in relation to creditworthiness assessment, due to:

- It is necessary for entering into and for the performance of the contract between you and the Bank, and
- It is authorised by Union and Member State law to which the Bank is subject.

This assessment is conducted on the basis of both internal data from your application and external data from credit scoring agencies. You have the right to human intervention related to this process, to express your point of view and to contest the Bank's decision based on credit scoring. Should you be rejected for reasons of creditworthiness, you have the possibility to contact the Bank via one of the contacts in Section 8 for providing an individual assessment.

7.7.2 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.

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.

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@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, Luxembourg.

9 WHERE CAN YOU FILE A COMPLAINT?

Should you wish to lodge a complaint at a supervisory authority, you can contact CNPD, based in Luxembourg (https://cnpd.public.lu/en/particuliers/faire-valoir.html).