DATA PROTECTION NOTICE

14 May 2024

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 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, 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. Our 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 may 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 in case of application: 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): copy of identity document, copy of passport, residence permit, salary certificate, 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) Correspondence, e.g. by telephone, e-mail, letter, contact form, information on the Bank's contractual relationship.
f) Data relating to your online account (username, IP address).
g) Information relating to your creditworthiness.
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.

Please note that as part of the Bank's application process in some of the Bank's markets, based on your consent, the Bank also compares your facial image with the photo of your identity card for identification purposes ("facial recognition"). The video image produced in this process is biometric data, and as such, it is sensitive under the GDPR.

Most of the above data categories are collected directly from you, with the following exceptions:

- Your account information and correspondence with the Bank are generated during the business relationship.
- Data relating to your online account are collected during your online presence.
- Data from credit scoring agencies (ref. Section 7.7.1).
- Data related to the KYC/AML checks.

With the exception of biometric data for identification purposes, the Bank does not ask you for any other sensitive personal data, nor do 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 DO WE PROCESS YOUR DATA?

3.1 Based on your consent

Depending on the market, you may provide the Bank with your explicit consent for facial recognition right before the video identification starts during your application on a specific page dedicated for this purpose (Article 9(2)(a) GDPR).

You may provide the Bank with your consent for marketing purposes by ticking a checkbox on the Bank's website when applying for the Bank's products (opt-in), allowing the Bank to inform you in the future by telephone, SMS, or email about offers, as well as about other financial and insurance services brokered by the Bank (Article 6(1)(a) GDPR).

3.2 To fulfil contractual obligations

Please note that most of the personal data listed in Section 2, excluding data related to the KYC/AML checks, are necessary for the Bank's contractual relationship and for providing services to you (Article 6(1)(b) GDPR), and for the purposes below. 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.

- Issuing a qualified electronic signature ("QES").
- The examination and acceptance of your respective application.
- Processing of customer enquiries.
- Payment execution.
- Residual debt insurance (explained in more detail in the respective data protection notices).
- Management of calls and follow-up.
- Execution of transactions.
- Provide bank statements.
- The execution of the services the Bank provides to you.
- 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.
- Communication with the credit scoring agency.
- Identity and age verification.
- Fraud prevention.
- Anti-money laundering and counter-terrorist financing.
- Obligations under tax law, including control and reporting.
- Risk assessment and management of the Bank.

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):

- Assessment of your creditworthiness after the conclusion of your contract for the purpose of potentially increasing your credit limit.
- 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.
- Occasional analysis ("one-off tests") of larger volumes of customer data provided by credit scoring agencies for the purpose of optimising our model for creditworthiness assessment.
- Advertising or market and opinion research.
- Assertion of claims/demands and defence in legal disputes.
- Ensuring the Bank's IT security and IT operations.
- Further development of services and products.
- Measures to assess risk factors for the Bank.
- Information to creditors or insolvency administrators requesting enforcement or attachment.

4 WHO CAN ACCESS YOUR DATA?

To achieve some of the purposes described in this Data Protection Notice, the Bank may, if needed or required, share your personal data with:

- Credit scoring services (specific to your country).
- Insurance company (AmTrust, EU).
- Call centres to ensure communication with you and to process your inquiries (based in Croatia, Serbia, Turkey, Bosnia and Herzegovina).
- IT and telecommunications services necessary for the secure storage of your data.
- A payment system which connects credit card transactions between the merchant, the merchant bank and the card-issuing bank (Mastercard, EU and US).
- Transaction system as an internal billing system for all transactions made, for calculating fees, interest, credits, and other credit card charges (EU, UK and USA).
- Embossing service to personalisation and production of credit cards (EU).
- Delivery services necessary to provide you with your credit card and other documents (DHL and Deutsche Post AG).

- Printing, scanning, archiving for creating and archiving customer communications, billing, bank statements (EU).
- Debt collection agencies (EU).
- Facial recognition and QES service providers (depending on the market where you are applying).
- Public bodies and competent authorities (e.g. CSSF, tax authorities, law enforcement authorities) for compliance with legal obligations and upon request.
- B2B partners (if you applied for a credit card via one of the Bank's B2B partners).

For the purpose of verifying your identity and assessing creditworthiness in the context of the Bank's business relationship, the Bank communicates with credit scoring agencies.

5 INTERNATIONAL DATA TRANSFERS

International data transfers mean for example transmitting personal data from the European Economic Area (EEA) to a country outside the EEA.

Please be informed that, where possible, the Bank aims to choose services that are based in the EU, with special regard to IT services. 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 to safeguard your rights. Regarding commercial organisations based in the US, since the adoption of EU-US Data Privacy Framework ("DPF"), the Bank aims to conclude contracts with US companies that are indicated as active on the DPF List when possible.

In addition, the Bank relies on Standard Contractual Clauses with regard to the Bank's call centres that are located outside the EU.

6 HOW LONG IS YOUR DATA STORED?

If you are an applicant to the Bank's services, your personal data will be retained for 5 years following your application.

If you are already one of the Bank's customers, the Bank retains your personal data during the Bank's 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 up to 10 years after the end of the Bank's business relationship in accordance with the Bank's legal obligations with regard to AML/CTF.

Please note that, exceptionally, this period may be longer in case the personal data is necessary for up to 30 years in case of civil litigation.

If your data is no longer required for the fulfilment of the Bank's contractual or legal obligations, it is deleted on a regular basis. Furthermore, you may exercise your right to erasure ("right to be forgotten") as explained below.

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 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. The Bank recommends exercising this right by calling the Bank to facilitate your request. 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.
- 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

Facial recognition is necessary for entering into a contract with the Bank in some of our market, for example Austria, Italy or Germany.

The facial recognition solution is provided by Netheos, a sub-contractor of Namirial, with the purpose of verifying your identity. For this, an image of you and your identity card is required, which are considered biometric data under the GDPR. These data will only be processed based on your explicit consent.

Please also note that a video recording is saved for the purpose of developing the AI technology of Netheos to provide you with an accurate identification service, which is necessary for you to be able to enter into a contract with the Bank. In addition, the Bank stores these video recordings for compliance with legal obligations related to AML/CTF.

You have the right to human intervention related to this process. Should you be rejected due to technical difficulties with the facial recognition, you can contact the Bank. The Bank will provide you with the necessary assistance to finish your application.

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.html).