

DATA PROTECTION NOTICE FOR SERVICE PROVIDERS AND BUSINESS INTRODUCERS

Summary

Data protection is of the utmost importance to Andbank Luxembourg (the “**Bank**”).

As required by the General Data Protection Regulation (EU) 2016/679 of the European Parliament of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the “**GDPR**”) and the Law of 1st August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters, this Service Provider data protection notice (this “**Service Provider Notice**”) shall provide you with a transparent overview of the Bank’s data protection policies and with information on how your personal data will be processed before and after entering into a contractual relationship with the Bank.

The “**data controller**” is defined as the natural or legal person, which, alone or jointly, determines the purposes and means of the processing of personal data. Andbank Luxembourg is data controller for the purpose of the contractual relationship.

The Bank will process personal data in compliance with the GDPR principles as laid down in chapter two of the regulation, namely:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimization;
- accuracy;
- storage limitation;
- integrity and confidentiality.

Your rights as a data subject in connection with personal data are:

- rights of access;
- right to correction;
- right to erasure;
- right to request the restriction of processing;
- right to transfer (data portability);
- right to object;
- right not to be subject to a decision based solely on automated processing, including profiling;
- right to withdraw consent for any processing specifically based on consent.

For any questions in relation to the processing of personal data or the exercise of its rights, you may contact the Data Protection Officer (“**DPO**”) via postal address at the Bank’s registered office, by phone + 352 27 49 76 1 or by email at dpo@andbank.lu.

You also have the right to make a complaint at any time to the National Commission for Data Protection (*Commission Nationale de Protection des Données* “**CNPD**”) <https://cnpd.public.lu/en/support/contact.html>.

1. Scope

This Service Provider Notice applies to all service providers and third parties with whom we had or currently have business relations with, including any natural persons acting as representatives of the legal entity, for example, notably business introducers (the “**Data Subject**”).

2. Regulations and Definitions

The applicable regulations are the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the “**GDPR**”) and the Luxembourg laws, notably the Law of 1st August 2018 on the organization of the National Data Protection Commission and the General Data Protection Framework.

2.1. Personal data and data processing

“**Personal data**” is defined as any information relating to an identified or identifiable natural person.

“**Data processing**” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.2 Data controller

Andbank Luxembourg (we), collect and process your personal data and act accordingly as data controller. As part of our responsibilities as data controller, we maintain a record of all processing activities in a data protection inventory (“**DPI**”) in accordance with article 30 GDPR.

2.3 Data processors

“**Data processor**” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller, i.e. persons or entities to whom the Bank sends data.

The Bank’s main data processors are further detailed in Appendix I of this Service Provider Notice.

2.4 GDPR principles

We process your personal data in compliance with the GDPR general principles as laid down in chapter 2 of the regulation, namely:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimization;
- accuracy;
- storage limitation;

- integrity and confidentiality

3. Personal data that we collect

We notably collect the following personal data:

- biometric data: your specimen signature or on an electronic signing pad for any invoices or service agreements signed with the Bank.
- official identification data: name, gender, title, date and place of birth, address (utility bill), contact details, identity card or passport information, nationality, country of residence for AML onboarding purposes;
- images when entering the Bank's premises recorded under the video surveillance protection system. (Further information is available in the video surveillance notice available on the Bank's website and upon demand, at its premises).

3.1 Sources from which we collect your personal data

The Bank collects the personal data from the following sources and at the following times:

- personal data provided in any exchanges when a service provider or business introducer is being onboarded before the service agreement is signed with the Bank.
- personal data accessible from AML name screening software such as OFSAA at any time during the contractual relationship.
- personal data accessible from publicly accessible sources, such as the Chamber of Commerce and Professional Registers, Google, LinkedIn etc at any time during the contractual relationship.
- personal data from the Bank's video surveillance system at its office premises.

For a detailed description of the categories of personal data processed and the third parties with whom we share the data, please see **Appendix I** of this Service Provider Notice.

3.2 Lawfulness and purpose(s) for processing

Any personal data that the Bank collects shall only be processed on one or more of the following lawful grounds (in accordance with article 6 GDPR):

- Where the data processing is necessary for the performance of a contract to which the Service Provider is party;
- Where certain data processing is necessary for the compliance with a regulatory obligation to which the Bank is subject (e.g PSD2 or AML regulations);
- certain data processing is necessary for the purposes of the legitimate interests pursued by the controller.

The Bank's data processing activities shall be limited to the specific purposes identified in **Appendix I**.

3.3 Personal data processed based on consent

The personal data detailed in row 2 in **Appendix I** will be processed on the basis of your consent.

You have the right to withdraw consent at any time in accordance with article 7 GDPR by notifying the Data Protection Officer through the contact information detailed below. Your withdrawal of consent may however necessitate the termination of your business relationship with the Bank, where inextricably linked to your contractual relationship with the Bank.

4. Professional Secrecy and Outsourcing

The Bank is obligated to keep all information confidential as it is bound by a duty of professional secrecy under article 41 of the law on the financial sector 1993. Any violation of this duty would incur specific penalties laid down in article 458 of the Luxembourg Penal Code.

Where the Bank outsources certain activities to an affiliated company in the Andbank group or a third-party service provider, it imposes confidentiality obligations on those entities accessing or processing confidential information. Particularly in cases where third party service provider is not regulated in Luxembourg, the description and purposes of the outsourced functions, the confidential information that may be transferred and/or disclosed to such Service Providers, and the country of establishment will be updated in the dedicated “Outsourcing” section in **Appendix I** of this Service Provider Notice.

5. Security measures

In order to protect your personal data the Bank implements:

- (i) technical and organizational measures, notably:
 - A. pseudonymization (to the extent it is necessary and technically feasible) and data encryption;
 - B. internal procedures and mechanisms such as the limitation of access on a “need to know” basis in order to ensure the ongoing confidentiality and integrity of the data;
 - C. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - D. regular testing and review of the effectiveness of technical and organizational measures for ensuring the security of the processing,
- (ii) regular training on data protection laws of all staff,
- (iii) robust contractual stipulations and follow up with the service providers to ensure that the data processors demonstrate and implement a similar level of data protection,
- (iv) policies and procedures to deal with any suspected data security breach, notifying the Data Subject and the CNPD (as defined below) of any suspected breach where legally required.

5. International transfers of personal data

When the data processing implies data transfers to countries outside of the European Economic Area (EEA) we take the necessary measures to protect your personal data.

To this end, we rely on:

- (i) International data transfer assessment: such assessment is performed before carrying out any international data processing activity;
- (ii) We adopt the following appropriate safeguards:
 - a. We will only transfer your personal data to countries that are deemed to provide an adequate level of protection for personal data by the European Commission. For further information, the most up to date list of countries benefitting from an adequacy decision is available on the EU Commission's website: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; or
 - b. Where the recipient country is not subject to an adequacy decision, we will use standard contractual data protection clauses approved by the EU Commission or one of the special derogations indicated in article 49 GDPR.
- (iii) We adopt technical and organizational measures (in accordance with article 32 GDPR), and as mentioned in point 5.

For the avoidance of doubt, Andorra benefits from an adequacy decision by the European Commission.

6. Data Retention

As the Bank commits itself to complying with all GDPR principles, in particular the purpose limitation and storage limitation principle, we shall retain your personal data for the period required in order to comply with applicable laws and regulations. In all cases, it is retained for no longer than the period necessary to carry out the designated purpose(s).

7. Data Subject's rights

Your rights in connection with your personal data are:

- Rights of access: you have the right to obtain from us confirmation as to whether or not personal data concerning you is being processed (art. 15 GDPR);
- Right to correction: you have the right to obtain from us, without undue delay, the rectification of inaccurate personal data (art. 16 GDPR);
- Erasure ('right to be forgotten'): you have the right to request the erasure of personal data concerning you without undue delay when it is possible and not in contradiction with other legal obligations (art. 17 GDPR);
- Restriction: you may request the restriction of processing notably when the processing is unlawful or if you have doubts on the accuracy of the information processed (art. 18 GDPR);
- Transfer (data portability): under certain circumstances you may ask to receive the personal data concerning you, in a structured, commonly used and machine-readable format and you also have the right to transmit those data to another controller (art. 20 GDPR);

- Right to object: you have the right to object, on grounds relating to your particular situation, at any time to processing of personal data (art. 21 GDPR); and
- Right to withdraw consent: you have the right to withdraw your consent at any time (art. 7 GDPR). Withdrawal of consent may however result in the impossibility for the Bank to pursue the contractual relationship thereof.

Your above-mentioned rights can be exercised by contacting the DPO as detailed below.

8. Contacts related to your data protection rights

For any questions in relation to the processing of your personal data or the exercise of your rights you may contact the Data Protection Officer (“DPO”) at + 352 27 49 76 1 or by email at dpo@andbank.lu.

You also have the right to make a complaint at any time to the National Commission for Data Protection (*Commission Nationale de Protection des Données* (“CNPD”) <https://cnpd.public.lu/en/support/contact.html>).

9. Changes to Notice

Any updates to this Service Provider Notice will be published on the Bank’s website which can be accessed at any time.

Upon material changes, we shall communicate the changes to you via e-mail.

Appendix I – Main Data Processing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) ⁵	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
1	Your identification data (name, nationality, date of birth), and any other information requested by the Bank, including data pertaining to convictions and offences and on the holding of a public office or political mandate, will be processed by the Bank and, where necessary, shared with regulatory authorities.	AL ¹ Compliance ABAR ² Opexia ³ Regulatory authorities and public officers including the Commission de Surveillance du Secteur Financier “CSSF”, financial intelligence unit “FIU”, cellule de renseignement du parquet “CRF”, or any public officers.	To conduct “Know Your Service Provider and Business Introducer” due diligence checks and to combat money laundering and terrorist financing as part of our regulatory obligations.	We outsource the maintenance of AML related applications to ABAR (i.e Namebook, OFSAA, EastNet) which is established in Andorra; We outsource AML reporting services to our provider, Opexia, which is established in Luxembourg.	Legal obligation under the Law of 12 November 2004 on the fight against money laundering and terrorist financing; Contract
2	Video surveillance recording of when you enter and exit the Bank premises.	AL authorized management and HR; Our surveillance service provider, G4S ⁴	To maintain physical security and limited access to the Bank’s premises.	N/A	Legitimate interest.

Appendix I – Main Data Processing Activities

¹AL refers to Andbank Luxembourg SA, with registered office at 4, rue Jean Monnet, L-2180 Luxembourg.

²ABAR refers to Andorra Banc Agrícola Reig SA, with registered office at Manel Cerqueda Escaler, 6, Escaldes, Andorra. AL's IT system and backups of the system are hosted and managed by ABAR.

³Opexia S.A. a PSF, supervised by the CSSF, with registered address 4, Rue Henri M. Schnadt, 2530 Luxembourg.

⁴G4S, with registered address at 14, Rue du Père Raphaël, L-2413, Luxembourg.

⁵Service providers are listed for indicative purposes and should also concern any appointed successor(s).