

## DATA PROTECTION NOTICE FOR CLIENTS

### 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 client data protection notice (this “**Client 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 throughout your relationship with the Bank (at the initial account opening request, once the account is opened, and after the account is closed).

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 with the client.

The Bank will process the client’s 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 client’s consent.

For any questions in relation to the processing of the client’s 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](mailto: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 Client Notice applies to all prospects, clients and their affiliates (the “**Data Subject**”). The term “affiliate” notably encompasses all natural persons or legal representatives (where the client is a legal entity), including its beneficial owners, proxyholders, auditors, domiciliary agent, service providers, and any other natural person or legal representative who has been granted a power of attorney on the client’s account.

## 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 1<sup>st</sup> 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 Client data.

The Bank’s main data processors are further detailed in Appendix I of this Client 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

The type of personal data we collect and process may vary depending on the nature of the services for which our clients have subscribed hereto, or any other agreements made with the Bank.

We notably collect the following personal data:

- biometric data: your specimen signature or on an electronic signing pad, data provided with your biometric passport;
- recordings of phone conversations with private bankers and treasury department.
- 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;
- socio-demographic data: information on family situations, notably whether the client is married and has children;
- banking, transaction, financial and fiscal data: type and quality of assets deposited with the Bank, any other bank or insurance company, knowledge of the financial assets, educational background, career and employment data;
- electronic identification information or any other data relating to your use of the Myandbank homebanking and online banking: connection data, IP address, mobile phone number, e-signature;
- video recordings when entering the Bank's premises (further information is available in the video surveillance notice available on the Bank's website and upon demand, at its 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**.

#### 3.1 Sources from which we collect your personal data

We collect your personal data from the following sources and at the following times:

- any personal data provided to the Bank via any exchanges at the account opening, during any ancillary service or activity conducted throughout the business relationship, and after the closing of the account.
- any personal data provided to us by any referee, business introducer or tied agent.
- personal data accessible from AML name screening software such as OFSAA.
- personal data accessible from publicly accessible sources, such as the companies and trade register, chamber of commerce and professional registers, Google, LinkedIn etc.
- personal data contained in the Bank's video surveillance system when you visit the entrance of our office premises.
- personal data exchanged from the Bank's telephone recording system.

- any other personal data sent after the opening of the account and throughout the business relationship via paper or electronic correspondence.

### 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 client is party;
- Where certain data processing is necessary for the compliance with a regulatory obligation to which the Bank is subject (e.g PSD2, AML, MIFID and market abuse regulations);
- certain data processing is necessary for the purposes of the legitimate interests pursued by the controller; and
- certain data processing is based on your consent obtained in writing in the account opening stage, or thereafter.

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 rows 2, 4, 6, 7, 8, 10, 11, 12, 13, 14, 20, and 25 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 Client 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.

## 6. 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](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.

## 7. 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, and in all cases, for no longer than the period necessary to carry out the designated purpose(s) (e.g proper account maintenance, facilitating client relationship management, and responding to legal claims or regulatory requests).

For most documents relating to accounts, the Bank retains most of the personal data for a period of ten years after the last exchange related to the prospect's request to open an account and ten years from the date of closure of the client's account.

## 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](mailto: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 Client 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 (if you are an existing client) via E-Andbank.

## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
1	Any personal data provided at account opening and throughout your banking relationship (notably identification data: name, birth date, nationality, family status, contact details, and financial data: origin of funds, tax identification number etc.).	AL <sup>1</sup> private department; client's third party introducer.	To provide banking and/or ancillary services by executing client instructions, and where applicable, maintain a relationship with your authorized client introducer.	N/A	Contract
2	Any personal data visible in your account is shared with third party(ies) to whom you have granted a power of attorney.	Any natural person or representative of a legal entity who has been granted a power of attorney by the account holder.	To execute the requested access rights of your account to the proxyholder as defined in any power of attorney granted by the client.	N/A	Consent (in the power of attorney); Contract.



## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
3	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 compliance department; ABAR <sup>2</sup> compliance department; Opexia <sup>5</sup> 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 Client” 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.
4	We share certain financial data about your security order (security type and pricing), and identification data (an electronic identification number) and where operationally required, your name, with ABAR in order to settle security orders.	AL dealing room; ABAR treasury department.	To settle security orders and financial instruments (i.e FOREX, fixed income, client deposits, commodities, futures and operations etc.).	We outsource certain back office activities to ABAR, including part of the settlement of security orders and reconciliation of clients’ securities positions.	Contract; Consent
5	Where you are a financial counterparty to any derivative trades, we share with ABAR and the designated trade repository, your unique identification code in order	ABAR; DTCC Derivatives Repository Ltd. <sup>6</sup>	To conduct EMIR reporting as part of our regulatory obligations.	We outsource certain back office activities to ABAR, including the reporting of certain derivative trades under EMIR to the designated trade repository, DTCC	Contract; Legal obligation under Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on



## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
	to comply with EMIR reporting requirements.			Derivatives Repository Ltd. which is established in the United Kingdom.	OTC derivatives, central counterparties and trade repositories to conduct EMIR reporting (notably, the data listed in Annex I of Commission Delegated Regulation (EU) 2022/1855 of 10 June 2022).
6	Your personal and financial data is stored in several business applications as part of the outsourcing of IT services to our third party IT service providers.	AL IT, private, investment desk, compliance, risk, finance, internal audit departments; IT ABAR; IT service providers based in the EEA.	To provide you with core banking and/or ancillary services.	We outsource IT operations, notably the infrastructure, maintenance and backups of the IT system, security measures, and the maintenance of several business applications to our parent company, ABAR, which is based in Andorra. We also outsource the technical functionalities, notably the consultation accesses and API in relation to our homebanking application, to our service provider Luxhub <sup>7</sup> , which is based in Luxembourg.	Consent; Contract
7	Your personal and financial data may be stored and backed up on a cloud by our cloud service providers which host their data centres in the European Economic Area (EEA).	Cloud service providers based in the EEA (e.g Microsoft 365 cloud <sup>8</sup> and Google cloud platform <sup>9</sup> )	To provide you with core banking and/or ancillary services.	Cloud solutions are outsourced to third party cloud providers in relation to business applications involving email communication and exchanges (e.g Microsoft Office), and the placement of client orders (e.g PAM).	Consent; Contract

## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
8	Your identification data (name) and financial data (IBAN, balance transferred) pertaining to each payment transaction is transferred to service providers acting as correspondent bank or otherwise involved in the transmission or execution of the payment order.	Service providers and correspondent banks, mainly: Society for Worldwide Interbank Financial Telecommunication (SWIFT); ABAR; ABS <sup>3</sup> ; Allfunds <sup>10</sup> ; BNY Mellon <sup>12</sup> ; BCEE <sup>13</sup> ; BCL <sup>14</sup>	To execute cash payment and security orders as part of our ancillary services provided, and in accordance with client instructions.	N/A	Consent; Contract
9	Where our reporting obligations are triggered, your identification and financial data relating to a payment order (i.e payee name, VAT and TIN number, account ID, date and time of transfer, currency, amount, location data of payer) will be shared with our service provider, ABAR, and the CESOP database.	AL IT and operations; ABAR operations; Central Electronic System of Payment information (CESOP) database.	To combat e-commerce VAT fraud in accordance with our CESOP reporting requirements.	N/A	Legitimate interest; Legal obligation to conduct the reporting under Council Directive (EU) 2020/284 as transposed by the Luxembourg Law of 26 July 2023 regarding the introduction of certain requirements applicable to payment service providers.
10	For fund / securities distribution services or where we act as Nominee Investor, your contact details (e-mail) will be shared with the intermediary acting as fund manager or broker in order to enable them to	AL operations; ABAR; ABS; Allfunds; Allfunds Spain <sup>15</sup> .	To allow certain specialized intermediaries to provide you with mandatory information about the	N/A	Contract; Consent

## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
	send you mandatory (tax) information about the fund / security.		fund or security that you have subscribed to.		
11	For fund / securities distribution services your personal data relating to direct and indirect beneficial ownership information of the aforesaid securities and data relating to the source of the funds is shared with marketing intermediaries involved in the transmission or execution of a specific transaction.	AL operations; ABAR; Allfunds; Allfunds Spain; Other marketing intermediaries that we may contract with.	To allow the marketing intermediaries to comply with their AML obligations.	N/A	Legitimate interest; Consent.
12	Prior to opening a credit facility, your financial and personal data provided to the Bank shall be processed to assess your creditworthiness and repayment capacity, and to consider the enforcement or application of sanctions in accordance with the credit's terms and conditions in the dedicated committee, which is subsequently then shared with our parent company, ABAR.	AL risk management; AL legal; AL authorized management; ABAR global risk management.	To conduct the necessary credit analysis in order to contract certain financial products and services and enforce its terms and conditions.	N/A	Legal obligation to monitor and report to management under the EBA/GL/2020/06 locally transposed in the CSSF circular 22/824; Contract; Consent.
13	Your financial data (i.e credit exposure, assets) and identification data (i.e name, place of residence, behavioral data) relating to your credit operations is regularly processed internally to monitor	AL risk management, authorized management, private department; global risk department of ABAR.	To perform the global credit risk monitoring function of the Andbank group, we send daily risk reports internally to our authorized management,	N/A	Consent; Legitimate interest to assess credit worthiness; Legal obligation to monitor and report to management under the EBA/GL/2020/06

## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
	credit irregularities (i.e overdrafts, matured credit lines).		and externally, to our parent company.		locally transposed in the CSSF circular 22/824; Contract.
14	Your financial data and personal data contained in the daily reports regarding all risks at the bank (notably credit risk, country, counterparty risk, market risk etc.) are shared with our management and our parent company, ABAR.	AL authorized management, dealing room, operations, finance; global risk department of ABAR; global finance department of ABAR.	To regularly report all banking risks on a daily basis internally, to our management, and externally, to our parent company, as part of our lines of defence in terms of internal governance.	N/A	Consent; Legal obligation to establish lines of defence as part of our governance requirements under CSSF Circular 12/552; Contract
15	Your financial and identification data is shared with certain regulatory authorities in order to comply with regulatory reporting requirements (daily liquidity reports, monthly and quarterly prudential reports, annual risk reports, bi-annual recovery plan reports).	AL risk management, compliance, and finance; Opexia; CSSF; BCL.	To comply with our legal reporting requirements under the CRR and CRD.	We outsource the performance of certain prudential reporting obligations to our service provider, Opexia, which is established in Luxembourg.	Legal obligation under the “CRR” or Regulation (EU) No 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms; and the “CRD” or Directive 2013/36/EU of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms; Contract (with our service provider).

## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
16	Your personal identification data (i.e name, address) and credit card contract information is shared with ABAR in order to deliver your credit card and PIN by post.	AL operations; ABAR	To deliver your credit card and the dedicated PIN code.	N/A	Contract; Legitimate interest.
17	Your financial data (assets in your account) and tax information is shared with direct tax administration ( <i>administration des contributions directes</i> ) in cases where there is a tax inquiry or summons ordering payment of an outstanding amount.	Luxembourg tax authorities ( <i>Administration des contributions directes</i> )	To execute a tax summons payment order encumbered on the Bank.	N/A	Legal obligation under Directive 2010/24/EU of 16 March 2010 concerning mutual assistance for the recovery of claims relating to taxes, duties and other measures and art. 8 of the Law of 27 November 1933.
18	Where you are a corporate client, your VAT, corporate income tax information, and identification data (name, nationality, location data), will be shared with our tax advisor providers and reported to the Luxembourg tax authority.	Luxembourg tax authorities ( <i>Administration des contributions directes</i> ) ; Our tax advisor, Deloitte <sup>16</sup>	To comply with VAT tax reporting requirements.	N/A	Legal obligation under Law of 12 February 1979 on VAT and General Tax Law of 22 May 1931.
19	If you are a Spanish tax resident, your financial data (open accounts of clients residing in Spain, information regarding loans and credits relating to immovable property) will be shared with the Spanish Tax Authorities.	Spanish Tax Authorities ( <i>Agencia Estatal de Administración Tributaria</i> )	To comply with Spanish tax reporting regulations.	N/A	Legal obligation under Real Decreto 253/2025 and Orden HAC/747/2025, de 27 de Junio 2025.

## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
20	Your personal data and financial data contained in your account will be shared with employees of ABAR, ABAR Gestio, and ABS (our sister company) if you have subscribed to discretionary portfolio management services (“DPM”).	AL discretionary portfolio manager; ABAR Gestio <sup>4</sup> ABAR; ABS.	To provide DPM services that render the client’s interests in an efficient and advantageous way with the support of our affiliated companies in the Andbank group.	N/A	Consent; Contract.
21	Any personal data you provide in a telephone call with your private banker or our dealing room staff in the context of a client order is recorded in our IT systems for the sole purpose of ensuring the correct execution of transactions.	AL operations; AL IT.	To comply with the MiFID II Directive requirement to monitor the correct execution of transactions concluded when dealing on own account, and for the reception, transmission and execution of client orders. This data is not accessed for any other purpose.	N/A	Legal obligation under MiFID II Directive 2014/65 as transposed in art. 37-1(6a) Law of 5 April 1993 on the financial sector; Legitimate interest: internal control purposes.
22	Your identification data and financial data relating to your accounts may be shared with certain judicial authorities upon their request (notably in the context of an account preservation, freezing order, liquidation order)	National and international judicial authorities, appointed liquidators and receivers ( <i>curateurs</i> ) in the case of liquidation or bankruptcies.	To comply with judicial requests and orders.	N/A	Legal obligation under Regulation (EU) No. 655/2017 of the European Parliament and of the Council establishing a European Account Preservation Order for the attachment of bank accounts

## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
23	Your identification data contained in certain documents may be shared with Luxembourg or EU based notaries in the case of administration of inheritance, special credit operations, or any other service rendered by the Bank which requires the notary's intervention (e.g notarization).	Notaries established in Luxembourg or, where necessary, other countries.	To perform ancillary services such as administration of inheritance or special credit operations as agreed upon between the Bank and client.	N/A	Contract; Legitimate interest.
24	Video surveillance recording of when you enter and exit the Bank premises.	AL HR and our authorized management; Our surveillance service provider, G4S <sup>17</sup>	To maintain physical security and limited access to the Bank's premises.	N/A	Legitimate interest.
25	Your account number, country of fiscal residence, and an aggregate of the total number of financial assets is shared with the global finance of ABAR to conduct the monthly accounting closing process.	AL finance; global finance department of ABAR	To properly conduct the monthly accounting closing process with the support of our parent company.	N/A	Consent; Contract.
26	Your identification data (unique identifier of transaction allowing to link signed document, name of signatory, connection times, e-mail address, IP address, geolocation, authentication history), biometric data (if using QES), and behavioral data (i.e sent, viewed, signed, status of completion) is processed to execute the electronic signatures.	AL IT; IT ABAR; Appian <sup>18</sup>	To use a platform that facilitates the collection of electronic signatures for documents signed between the Bank and client.	We receive externalized support from our service providers and parent company to execute the e-signatures of clients.	Legitimate interest; Contract.



## Appendix I – Main Data Processing and Outsourcing Activities

Row	Data that we process	Data recipient (person or entity receiving the data) <sup>11</sup>	Purpose(s) for which we process or share the data	Outsourcing activity (where applicable)	Legitimacy for processing (article 6 GDPR)
27	For SEPA credit transfers, we share your IP address, Device ID, name, financial scoring, payment history data with our service provider in Spain in order to execute instant credit transfers in euro and to complete verification of payee obligations.	AL operations; Cecabank <sup>19</sup>	To provide instant credit SEPA transfers in euro and complete our verification of payee obligations.	We outsource the ICT aspects of the instant payment and verification of payee functions to Cecabank.	Contract; Legitimate interest; Legal obligation under Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 as regards instant credit transfers in euro.

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

<sup>2</sup> ABAR 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.

<sup>3</sup> ABS refers to Andbank Espana Banca Privada, with registered address at 22, Paseo De La Castellana, 28046 Madrid, Spain

<sup>4</sup> ABAR Gestio refers to ANDORRA GESTIÓ AGRÍCOL REIG, SAU, SGOIC, an entity incorporated under the laws of the Principality of Andorra whose registered office is at Carrer Manuel Cerqueda i Escaler, number 3-5, Escaldes-Engordany.

<sup>5</sup> Opexia S.A. a PSF, supervised by the CSSF, with registered address 4, Rue Henri M. Schnadt, 2530 Luxembourg.

<sup>6</sup> DTCC Derivatives Repository Ltd. with registered address Broadgate Quarter, 7th Floor, One Snowden Street, London, EC2A 2DQ.

<sup>7</sup> Luxhub SA, with registered office at 153155, rue du Kiem, 8030 Strassen, Luxembourg, registered with the Luxembourg Trade and Companies Register under number B223400 and duly authorized by the Commission de Surveillance du Secteur Financier (CSSF) to provide payment initiation and account information services in accordance with the PS Law.

<sup>8</sup> Microsoft 365 cloud refers to the Microsoft Azure cloud computing services provided by Microsoft Ireland Operations Limited, One Microsoft Place, South Country Business Park, Leopardstown, Dublin 18, D18 P 521, Ireland.

## Appendix I – Main Data Processing and Outsourcing Activities

<sup>9</sup> Google cloud platform refers to the cloud computing services provided by Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States.

<sup>10</sup> Allfunds refers to the Luxembourg branch of the Allfunds Bank S.A.U, which is duly authorised as a branch of a foreign bank supervised by the Commission de Surveillance du Secteur Financier (CSSF), with registered office, in 30 Bd Royal, 2449 Ville-Haute Luxembourg, Luxembourg.

<sup>11</sup> Service providers are listed for indicative purposes and should also concern any appointed successor(s).

<sup>12</sup> BNY Mellon, with registered address 240 Greenwich St New York, NY 10007 United States of America.

<sup>13</sup> BCEE refers to Banque et Caisse d'Épargne de l'État, supervised by the European Central Bank, with registered address, 1 Place de Metz, 1930 Gare, Luxembourg.

<sup>14</sup> BCL refers to Banque Centrale du Luxembourg, 2 boulevard Royal L-2983 Luxembourg.

<sup>15</sup> Allfunds Spain refers to Allfunds Bank S.A.U, a credit institution duly regulated by the Bank of Spain under number 0011 and authorised by the Spanish Securities Market Commission (CNMV) to act as a broker and fund distributor with registered office in Padres Dominicos, 7, 28050 – Madrid and registered in the “Registro Mercantil de Madrid” under (tomo 15,897, libro 0, sección 8, folio 17, página M568651).

<sup>16</sup> Deloitte Luxembourg with registered address at 20, Boulevard de Kockelscheuer, L-1821 Luxembourg.

<sup>17</sup> G4S General Services S.A. with registered address at 14, Rue du Père Raphaël, L-2413, Luxembourg.

<sup>18</sup> APIAN SOFTWARE INTERNATIONAL LLC as distributed by VASS Consultoría de Sistemas S.L Avenida de Europa 1, Edificio B, 28108, Alcobendas, Madrid, Spain.

<sup>19</sup> Cecabank S.A. registered under Code 2000 in the Register of Banks and Bankers of the Bank of Spain, and in the Mercantile Register of Madrid, under Volume 30,405, Book O, folio 57, Section 8, Sheet M-547,250, Entry 1. Its registered address Calle Alcalá, 27, MADRID (28014), with Tax ID Code A-86436011.