

PERSONAL DATA PROTECTION NOTICE

Legal framework

The Regulation (EU) 2016/679 of the European Parliament and 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to the processing of personal data and on the free movement of such data (through which the Directive 95/46/EC is repealed) (“GDPR”) and the related Luxembourg laws, notably the **Act of 1st August 2018** on the organization of the National Data Protection Commission and the general data protection framework and the **Act of 1st August 2018** on the protection of individuals with regard to the processing of personal data in criminal and national security matters, as may be amended from time to time (“the Law”).

Legal key points

- Strengthen the control of individuals over the processing of their personal data by notably offering the possibility for private individuals to request a right of access, rectification, objection and, where applicable, the deletion of their personal data.
- Increase responsibility for controllers
- More important role for data protection authorities
- Same rules in all 28 countries of the EU
- Directly applicable since 25 May 2018
- To all organisations processing personal data of EU residents on EU territory

The aim of this Personal Data Protection Notice (“PDPN”) is to present you how Andbank Luxembourg (“Andbank” or “the Bank”) processes the personal data (“Data”) of its clients or future clients, direct relationships and services providers/ vendors as well as natural persons affiliated to the Bank.

What is “personal data”?

Any information relating to an identified or identifiable natural person.

The Bank will only process clear Data, i.e. Data that allows the immediate identification of a client (not pseudonymised data or anonymised data).

For example, the Bank will process the following Data:

- Official identification Data (name, surname, date and place of birth, ID number, email address and IP address of your PC or mobile device)
- Education, training and qualification Data (level of education, professional qualification)
- Career and employment Data (employer’s name, remuneration)
- Transaction Data (such as your bank account number, deposits, withdrawals and transfers related to your account)
- Socio-demographic Data (such as whether you are married and have children)
- Online behaviour and preferences Data (such as IP address of your mobile device or computer and the pages you visit on the Bank websites and apps)

- Data relating to your habits and preferences
- Data contained in a duly completed form sent to our Bank
- Audio-visual Data (video surveillance or phone calls recording)
- Geolocation Data (showing locations of withdrawals and payments)
- Some Data from public sources or obtained from third parties (tax administration, courts or public prosecutor's office, data accessible on open networks such as website, blog, social networks, or obtained from press publications)
- Data collected from cookies

What is “sensitive data”?

Contrary to “Standard data”, which generally can be processed, sensitive Data (such as racial or ethnic origin, trade union membership, religious or philosophical beliefs, political opinions, health data, data on sex life, genetic data, biometric data, judicial data), by default, cannot be processed, unless we can invoke an exception foreseen by GDPR or the Law. Examples: express consent (restrictive interpretation), legal obligation in the field of Labour law, necessary to protect the vital interests of the data subject, etc.

What is “processing”?

Processing personal data can be any operation or set of operations on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The life-cycle of a processing activity is the following:

- Collection: it can be direct or indirect, automatic or manual, with or without consent.
- Use
- Conservation
- Deletion: either a simple deletion or an anonymisation.

Who is responsible for the processing of your Data?

The entity responsible for processing your data is the company limited by shares “Société Anonyme”, abbreviated into “SA”, Andbank Luxembourg (the Bank”), with business address at [4, rue Jean Monnet, L-2180 Luxembourg]. You may contact the Bank Data Protection Officer when deemed appropriate, at the abovementioned postal address, at the email address [dpo@andbank.lu] or by tel. + 352 27 49 76 - 1.

The Bank is accountable to the supervisory authorities that oversee compliance with Data regulations. The Bank shall determine the purposes for which the data are processed, as well as the means used and all of the features of the processing as explained in this PDPN.

Why and on which basis do we process your personal data?

The Bank shall collect and process your personal Data only for legitimate business reasons. This includes:

1 To comply with legal and regulatory provisions:

-Banking and financial regulations in compliance with which we:

- a) set up security measures in order to prevent abuse and fraud
- b) detect transactions which deviate from normal patterns
- c) define your credit risk score and your reimbursement capacity
- d) monitor and report risks that institutions could incur
- e) record, when necessary, phone calls, chats, e-mails

-Reply to an official request from a duly authorised public or judicial authority

a) public authorities, regulators and supervisory bodies such as the central banks of the countries where we operate

b) tax authorities may require us to report your assets (balances on deposit, payment or savings accounts or holdings on an investment account). We may process your social security number for this.

c) judicial/investigative authorities such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request

d) lawyers, for example, in case of bankruptcy, notaries, for example when answering to heirs, trustees who take care of other parties' interests, and company auditors.

-Prevention of money laundering and financing of terrorism

-Compliance with legislation relating to sanctions and embargoes

-Fight against tax fraud and fulfilment of tax control and notification obligations

2 To perform a contract with you or to take steps at your request before entering into a contract

We use your Data to enter into and perform our contracts with you including to:

a) Analyse your application in order to assess whether the envisaged contract can be concluded

b) Determine the conditions under which the contract could be concluded

c) Manage our products (deposits, credits, payment instruments, insurance) and our services (transaction execution of any type, advice, wealth management, insurance intermediary)

d) Manage our relationship with you

e) Provide you with information regarding our products and services

f) Assist you and answer your requests

g) Evaluate if we can offer you a product or service and under which conditions

h) Provide products or services to our corporate clients of whom you are an employee or a client

3 To pursue our legitimate interests

We use your Data in order to deploy and develop our products and services, to improve our risk management and to defend our legal rights and as well to:

- a) Keep proof of transactions
- b) Perform behavioural and transactional analysis in order to detect fraud
- c) Prevent personal injury and damage to goods
- d) Ensure the security of persons and property
- e) Perform IT management including infrastructure managements and business continuity and IT security
- f) Establish aggregated statistics, tests and models, for research and development, in order to improve the risk management of our Group or in order to improve existing products and services or create new ones
- g) Perform client satisfaction and opinion surveys
- h) Personalise our product and service offering by improving the quality of our banking, financial and insurance products and services and advertising products that match your situation and profile as defined by us

4 To respect your choice if we request your consent for specific processing

In some cases, we require your consent to process your Data, for example, where the above purposes lead to automated decision-making, which produces legal effects or which significantly affects you. At that point, we will inform you separately about the logic involved as well as the significance and the envisaged consequences of such processing.

After specifically requesting your consent, we may process your Data (mobile phone number and email address) to send you invitations to events and advertising or personalised offers as part of its direct marketing activities or via newsletters. If you no longer wish to receive electronic communications, the Bank gives you the possibility at any time to object to this processing of your Data (see section xx).

What do we do with your personal data?

We only use your personal data for legitimate business reasons, this includes:

- Administration (opening account process including verify your identity, obtain your address or phone number)
- Product and service delivery (to assess whether you are eligible for certain products or services (loan, investment, current or savings account, etc.)
- Managing customer relationships (we may ask you for feedback about our products and services and share this with certain members of our staff to improve our offering. We might also use notes from conversations we have with you online, by telephone or in person to customise products and services for you)

- Credit risk and behaviour analysis (to assess your ability to repay a loan when we apply specific statistical risk models based on your Data)
- Personalised marketing
- Providing you with the best-suited products and services
- Improving and developing products or services
- Preventing and detecting fraud and data security

For how long do we keep your personal data?

We will retain your Data for the period required in order to comply with applicable laws and regulations, or for the period defined by our operational requirements such as proper account maintenance, facilitating client relationship management, and responding to legal claims or regulatory requests. For instance, most client information is kept for the entire duration of the contractual relationship and for 10 years after the end of the contractual relationship.

Who we share your data with and why?

To be able to offer you the best possible services and remain competitive in our business, we share certain data internally and outside of the Bank. This includes:

- Service providers/vendors that perform services on our behalf
- Independent agents, intermediaries or brokers, financial institutions, banking and commercial partners with which we have a regular relationship (banks, insurance companies, debit and credit card issuers)
- Supervisory, financial, taxation, administrative or judicial authorities, state agencies or public bodies, upon request and to the extent permitted by law
- Certain regulated professionals such as lawyers, notaries or auditors
- Certain Andbank Group entities (in case of consolidated risk management for example)

Do we transfer your Data outside the European Economic Area?

As a result of our activities, the Bank may have to communicate data outside the EEA. For transfers to non-EEA countries where the level of protection has not been recognised as adequate by the European Commission, we rely on a derogation applicable to the specific situation (host of data in Andorra) and we take all adequate steps to guarantee that your Data are duly protected in the country of destination by ensuring, for example, that the protection of Data is guaranteed by suitable contractual provisions or by any other means that provides level of security.

Data security

Andbank shall take all the necessary steps to ensure the confidentiality, integrity, availability and robustness of the Data, the processing systems and services under its control and the security of their treatment pursuant to the legal requirements.

Our staff shall only access your Data if it is relevant to the performance of their missions. Our staff is bound by strict professional secrecy and must respect the confidentiality of your Data. Our offices as well as access to our servers and networks are tightly protected and we take great care when choosing our commercial suppliers and partners in order to ensure that any transfer or processing of Data by them is fully secure.

The Bank also establishes technical protection measures in order to offer an ever-higher level of security for your Data. These measures may entail the encryption of your Data and the installation of firewalls or anti-viruses.

You can help us to secure your Data by following these advices:

- Always perform updates on your browser or your mobile applications
- Never switch off the security features on your devices
- Make sure that a firewall is installed on your devices in order to continuously monitor the incoming and outgoing information flows
- Install a good anti-virus programme and make sure it is kept updated
- Secure your Wi-Fi connection
- Do not choose overly simple passwords
- Do not communicate your confidential passwords to third parties
- Report any potential fraud or misuse to your Bank

Which are your rights and how can you exercise them?

In accordance with applicable regulations, you have the following rights to:

Access and receive your Data: you can obtain information relating to the processing of your Data and a copy of such Data.

Rectify: where you consider that your Data is inaccurate or incomplete, you can require that such Data be modified accordingly. In order to keep your Data fully up-to-date and to provide you with a quality service, please notify us of any change of address, renewal of ID, etc. If we shared Data about you with a third party that is later corrected, we will also notify that party.

Object to processing: you can object to the processing of your Data on grounds relating to your particular situation. You have for example the absolute right to object to the processing of your personal data for direct marketing purposes, which includes profiling related to such direct marketing.

The Bank may however refuse this request on compelling grounds, particularly if the processing of the Data is needed, for example, for the purpose of preventing fraud. In such a case, this may lead to the Bank terminating its contractual relationship with you or refusing to perform an operation.

You cannot object to us processing your Data if we are legally required to do so (example : security issues with your account, such as when your card is blocked, even if you have opted out of receiving personalised commercial messages).

Object to automated decisions: we sometimes use systems to make automated decisions based on your personal information if this is necessary to fulfil a contract with you or if you gave us consent to do so. You have the right to object to such automated decisions (for example the price we charge for a product or service) and ask for an actual person to make the decision instead.

Restrict processing: you have the right to ask us to restrict using your personal data if i) you believe the information is inaccurate ii) we are processing the Data unlawfully iii) Andbank no longer needs the Data, but you want to keep it for use in a legal claim iv) you have objected to us processing your Data for our own legitimate interests

Data portability: you have the right to ask us to transfer our Data directly to you or to another company. This applies to personal data we process by automated means and with your consent or on the basis of a contract with you. Where technically feasible, we will transfer your personal data.

Delete: you can require the deletion of your personal data to the extent permitted by law, notably if i) we no longer need it for its original purpose ii) you withdraw your consent for processing it iii) you object to us processing your Data for our own legitimate interests or for personalised commercial messages iv) Andbank unlawfully processes your Data or v) a law of the European Union or a member state of the European Union requires our Bank to erase your personal data.

Withdraw your consent: where you have given your consent for the processing of Data, you have the right to withdraw your consent at any time. However, unless you terminate the contract between you Andbank, we may, after balancing your interests and its own interests, continue to process some of your Data.

You may submit your request via the different communication channels placed at your disposal by the Bank. You may also change your mind via these same means of communication.

Notwithstanding the foregoing, the exercise of your right of objection does not preclude Andbank from contacting you for reasons other than those stipulated above and, more precisely, in relation to a legal obligation or in order to perform a contract.

Complain: should you not be satisfied with the way we have responded to your concerns, you have the right to submit a complaint to us. If you are still unhappy with our reaction to your complaint, you can escalate it to the Andbank Data Protection Officer at the following e-mail address [dpo@andbank.lu] or by letter at [4, rue Jean Monnet, L-2180 Luxembourg.

In accordance with the Law, in addition to your rights above, you are also entitled to lodge a complaint to the National Commission for Data Protection “*Commission nationale pour la protection des données*” (cnpd.lu): Complain Service, 1, avenue du Rock’n’Roll L-4361 Esch-sur-Alzette - E-mail: info@cnpd.lu.

Your duty to provide Data

There is certain information that we must know about you so that we can start and execute our duties as a bank and fulfil our associated contractual duties. There is also information that we are legally obliged to collect. Without this Data, we may not be able to open an account for you or perform certain banking activities.

How we protect your Data?

We apply an internal framework of policies and minimum standards across all our business to keep your Data safe. These policies and standards are periodically updated to keep them up to date with regulations and market developments. More specifically and in accordance with the law, we take appropriated technical and organisational measures (policies and procedures, IT security, etc.) to ensure the confidentiality and integrity of your Data and the way it is processed. Moreover, Andbank employees are subject to confidentiality and may not disclose your Data unlawfully or unnecessarily.

How can you keep up with changes to this Personal Data Protection notice?

In a world of constant technological changes, we will update this PDPN regularly. We invite you to review the latest version of this PDPN online and we will inform you of any material changes through our website or through our other usual communication channels.

How to contact us?

If you have any questions relating to our use of your personal data under this PDPN, please contact our data protection officer by letter to Andbank Luxembourg, 4, rue Jean Monnet

L-2180 Luxembourg or by email to: dpo@andbank.lu. If you wish to learn more about cookies, please read our “Cookies Policy” available on our website andbank.lu.