



Privacy Statement

DELEN

PRIVATE BANK

The protection of your privacy is extremely important. This Privacy Statement contains detailed information about how we handle, collect, process, share and safeguard your personal data that we collect in the context of our services. It also tells you about your rights and choices with respect to your personal data, and how you can contact us if you have any questions or concerns.

Please read this Privacy Statement carefully. If you do not agree with this Privacy Statement or any part thereof, you should not use or request our services. If you change your mind in the future, you must stop using our services and you may exercise your rights in relation to your personal data as set out in this Privacy Statement.

1. We handle your personal data with due care

Delen Private Bank Luxembourg SA and its group entities¹ ("Delen Private Bank", "the Bank" or "we"), whose registered office is located at L-1150 Luxembourg, route d'Arlon, 287, is a credit institution specialized in discretionary asset management. The Bank acts as the data controller under the General Data Protection Regulation ("GDPR") for any personal data collected in this capacity. We always handle personal data with due care.

2. Scope

This Privacy Statement applies to the following persons:

- past, present or potential clients and agents;
- the representative / beneficial owner of legal entities that have a past, present or potential relationship with the Bank; and
- person involved in any transaction with the Bank, whether in his/her own name or in the capacity of a legal entity (e.g. legal representative, effective beneficial owner, etc.).

We obtain your personal data inter alia as follows:

- when you become a client of the Bank or when you share data with us during the course of our business relationship;
- when you take on another role on an account (e.g. as a proxy);
- when you accept an invitation of an event organized by the Bank;
- when you contact the Bank through one of our communication channels; and
- from third parties (e.g. beneficiary registers, financial databases such as the Central Individual Credit Register and MYMinFin, databases consulted for the purpose of combating money laundering and the financing of terrorism, social media such as LinkedIn, data brokers and data enrichment service providers such as Graydon, or traditional media).

3. Which personal data do we process?

The term "Personal Data" refers to any information relating to an identified or identifiable natural person.

If you are a client or potential client of the Bank, the Bank processes data such as:

- your identification data, such as first name and surname, date and place of birth, identity card number, address, nationality, specimen of your signature, tax number or national registry number, IP address and the type of mobile device or computer you use for our online applications;
- your contact details, such as your address, email address, telephone number, personal or professional number;
- your financial data, including account numbers, transaction data, credit records and overall asset situation;
- your family situation, e.g. marital status, family situation and relationships;
- your professional data, e.g. function, mandates in companies and associations;
- your patrimonial data, e.g. a marriage contract or donation documents or any information collected as part of the Delen Family Services;
- your areas of interest that you have communicated to us, such as preferred leisure activities;
- KYC identification data - 'Know your client';
- data related to the use of the Bank's digital applications;

¹ Excluding JM Finn & Co Ltd. and Cadelam NV.

- the images from our surveillance cameras, for security reasons our offices can be fully or partially placed under camera surveillance;
- the recordings of telephone and video calls may be processed for the purposes of internal controls, dispute management, or the continuous improvement of our services.

Sensitive data

The term 'Sensitive Data' refers in particular to data relating to health, ethnic origin, religious or political beliefs, genetic or biometric data or criminal data.

We collect sensitive data in the context of our KYC obligation and in the context of our specific services (e.g. estate planning).

KYC, which stands for 'Know Your Client', refers to all the procedures by which a bank can identify a client or a potential client. As part of our duty of care to our clients, we must comply with regulations on combating money laundering, preventing terrorist financing and tax fraud.

We apply a range of measures in this regard. These include the collection of personal data necessary to prevent and detect fraudulent behaviour and behaviour that violates national and international regulations.

In this context, we will also check certain data we have collected against public or external databases and we must also check, identify and record any data relating to sources of information that contain judicial or criminal data about the client.

We also need to check whether the client is a Politically Exposed Person (PPP).

When processing Sensitive Data, we always ensure we rely on a valid legal basis for processing under the GDPR, such as your explicit consent or when authorized by law.

Third party data

In certain cases, the Bank holds data on persons connected to you (e.g. when you share information or documents with us that relate to connected persons).

When you provide us with such information, we ask you to inform these persons about it and to notify them that we process the Personal Data concerned for the same purposes and under the same conditions as set out in this Privacy Statement.

Data on minors

We process data on minors to perform our contractual obligations, such as when you open an account for them or when you provide data on them in the context of our services, including in the context of Estate Planning or Delen Family Services

4. Why do we process personal data?

The Bank processes your personal data for the following purposes set out below. By 'processing' we mean all manual or automated operations that are performed on the data in question, such as the collection, recording, storage, consultation, adjustment, organisation, use, transfer or deletion.

- **In order to provide you with an adequate service.** We use your personal data to carry out our contractual obligations towards you by providing you with the Bank's services, including managing your accounts, executing transactions, estate planning and credit monitoring.
- **To communicate with you.** When we need to perform our contract with you or when it is in our legitimate interests, we will communicate with you about our services including by sending you announcements, reminders, updates, and support and administrative messages.
- **To improve our services.** We are continuously working to improve our services. We do this, for example, by offering training to our employees and by continuously developing our IT systems. The latter includes processing data to perform functionality tests, improve administrative tasks (e.g., drafting contact reports), and enable us to offer our services in a personalized way through categorization or the creation of insights. Additionally, the bank may process personal data to perform statistical analyses and tests. To protect your personal data, the bank will take the necessary measures to process the data in an anonymized or aggregated manner.
- **To protect against fraud and abuse.** It is in our legitimate interests to keep our services safe for our clients. We may use your personal data to prevent, detect, monitor and investigate abuse, fraud and other harmful, unauthorized or illegal activity.

- **To comply with legal obligations.** When we open an account for you, we are required by law to collect personal data to confirm your identity and to determine whether we can enter into a business relationship with you. We also have obligations under anti-money laundering and counter-terrorism legislation, obligations under financial markets regulations such as the MiFID II regulations, obligations under regulations relating to shareholders right such as SRD II, obligations under financial planner regulations and financial reporting obligations (e.g. to the Central Contact Point). To comply with these legal obligations, the bank may use systems that process data automatically.
- **Direct marketing.** Except where consent is required, and unless you have opted out of receiving marketing communications, it is in our legitimate interests to use your personal data to communicate with you regarding our products, services and other news, and contact you about products or services we think will be of interest to you. You can opt out of such communications by following the unsubscribe mechanism on any communication, or by otherwise emailing us at privacy-lux@delen.bank.
- **To enforce our Terms and Conditions relevant to the specific service, and to defend the Bank against legal claims or disputes.** Where it is in our legitimate interest to ensure the integrity of our services and to defend ourselves against legal claims or disputes, we will use the personal data relevant to such a case. Some processing may also be necessary as requested by any judicial process or governmental agency. In these circumstances, we will process your personal data to comply with a legal obligation or when it is in our legitimate business interests.

If, where we are processing your personal data to perform our contract with you, you do not provide the personal data, we may not be able to conclude or fulfill such contract.

5. How long do we store your personal data?

How long personal data is kept depends on the type of data. The Bank uses data when and for as long as it has a purpose to do so (for example, in the context of exercising a contract or on the basis of legal obligations on the part of the Bank). For the exercise of your or our rights, this can be longer than the statutory retention periods. This also allows us to offer you the best possible service, especially in the context of our KYC obligation and tax and Estate Planning services. If the statutory retention period is exceeded for a certain data, we take additional security measures to ensure its security.

6. Can data be shared with third parties?

In certain cases, we transfer certain data to third parties, both internal (within the group) and external recipients (i.e. outside the group). For example, this may happen to fulfil our obligations, on your request, to provide you with group content and services, marketing, or to improve your experience, products and other services. As part of our banking activities, the Bank may need to transfer personal data to countries located outside the European Economic Area (EEA). When doing so, we will ensure that relevant safeguards are in place to afford adequate protection for your personal data and we will comply with applicable data protection laws, in particular by relying on an adequacy decision by the European Commission, on contractual protections for the transfer of your personal data or a derogation if available.

Governmental, legal and supervisory authorities

In order to comply with our legal obligations, we must disclose certain data to governmental, judicial and regulatory authorities:

- public authorities and regulatory authorities and supervisors such as the FSMA or the National Bank of Belgium;
- the tax authorities may require certain reports from us, e.g. in the context of FATCA/CRS;
- the judicial / investigative services (police, prosecutor, courts and arbitration / mediation authorities) upon legal request; and
- the notaries, e.g. within the framework of a notarial deed or when processing inheritance files.

Bank J. Van Breda

Data may be provided by Delen Private Bank to Bank J. van Breda for clients or potential clients introduced by the latter. Bank J. van Breda may use these data among other things:

- to prevent misuse and fraud;
- to compile statistics and carry out tests;
- in the context of commercial services;
- when we act as a third-party pledgee; and
- to improve the quality of the services to the aforementioned clients.

Delen Group

Delen Private Bank provides IT; Information Security and Back Office services to other entities within the Delen Group. In this capacity, the Bank is responsible for processing personal data relating to clients and potential clients of all Delen group entities. Additional security controls are implemented to the data transferred in this scope. Delen Private Bank may use these data:

- to prevent misuse and fraud;
- to provide ICT that supports operational activities;
- to support regulatory reporting;
- to develop and improve Delen Group's services;
- to ensure security.

Financial institutions

When you make a transfer to an account at another bank, the transaction always involves an institution other than the Bank. For the settlement of securities and payment transactions, both nationally and internationally, we as the principal are required to provide the other financial institution with data relating to you, such as your name, your address and the account number.

In the context of money transfers or transactions in financial instruments, the data required to carry out the transactions is processed by third parties involved in the transaction (e.g. correspondent banks, stock exchanges, financial messaging service providers, etc.), which may be located outside the EEA.

Other Service Providers and third parties

The Bank may share information with third party advisors such as tax consultants and legal advisors. In some cases, these advisors may be indicated by you or proposed to you by the Bank, such as notaries, lawyers, accountants or auditors.

Furthermore, in the event that certain tasks are outsourced, the Bank may pass on data to carefully selected third parties who process certain data on the Bank's instructions. For this purpose, the Bank uses third party processors who, in the opinion of the Bank, offer adequate guarantees for the protection of this data. These third parties undertake to preserve the confidentiality of the data.

The following are non-exhaustive examples of external service providers the Bank may share your personal data with:

- Postal service providers and courier service providers, when managing correspondence with our clients (e.g. when communicating by post);
- Data brokers, online databases and data enrichment service providers, to better understand our customer base, to build and expand our database with client information and to organise direct marketing campaigns;
- Event planners and other event related service providers, when organising events;
- Archive and storage service providers, in the context of external archive management.

If the Bank is involved in a merger, acquisition or asset sale, financing due diligence, reorganisation, bankruptcy, receivership, sale of company assets, or transition of service to another provider, your personal data may be sold, transferred or otherwise shared including as part of any due diligence process.

7. Your rights and exercising them

You also have a number of rights concerning the personal data that the Bank processes. You will find an overview below:

- you can access and view your data;
- You can consult the personal data that we process about you and/or request a copy;
- you can have your data corrected;

In so far as the personal data that we maintain are incorrect or incomplete, you have the right to request that these data are corrected. If we have passed them on to a third party, we will inform this party of your request for correction.

- you can object to a certain use of your data

We will comply with this request unless the processing is necessary for legal purposes or to fulfil our contractual obligations.

For example, you can object to commercial messages being sent. When you become a client with the Bank, we may ask you if you want to receive invitations to our events. If you change your mind at a later date, you can stop the sending of these, in particular by contacting your relationship manager.

When we process personal data on the basis of your consent in the case of direct marketing, you always have the option of withdrawing your consent.

- you can have your data deleted

You can request that we delete it. We will comply with this request unless the processing is necessary for legal purposes or to fulfil our contractual obligations.

Exercising your rights

You can exercise your rights by sending a letter to Delen Private Bank Luxembourg, L-1150 Luxembourg, route d'Arlon 287, for the attention of the 'Data Protection Officer' or by sending an e-mail to privacy-lux@delen.bank.

In order to ensure the confidentiality and protection of your data, we can ask you for a copy of your proof of identity or additional information to verify your identity.

Any request for the exercise of a right that you make to the Bank will be dealt with and answered within the statutory time limit.

In some cases, we may refuse to comply with your request, or we may charge you a fee for processing your request, if it is deemed to be improper, repetitive, or if it results in excessive costs.

Should the Data Protection Officer decide that no action can be taken on a request, he or she will inform you no later than one month after receiving the request. In this case, the reason of the action will be provided to you.

Your right to lodge a complaint

If you do not agree with the Bank's position, you have the right to lodge a complaint. You can send this to the Data Protection Officer of Delen Private Bank Luxembourg via privacy-lux@delen.bank. You are also free to contact the Belgian Data Protection Authority via the details given below, or the data protection authority of your own country:

- by postal mail: Commission Nationale pour la Protection des Données, Boulevard du Jazz 15, L-4370 Belvaux
- via the website: <https://cnpd.public.lu/fr.html>.

8. How do we protect your personal data and what can you do to help us?

We take appropriate technical and organisational measures (policies and procedures, IT security, etc.) to ensure the confidentiality and integrity of your personal data and processing. To ensure the security of your personal data, we apply a number of internally developed policies and standards to all our activities. These are regularly updated to take into account the latest regulations and developments in this area.

For example, bank employees are subject to confidentiality obligations and must not disclose your personal data in an unlawful manner or when it is not necessary for the performance of their duties. To help us protect your personal data permanently, you should always contact the Bank if you suspect that your personal data has been misused.

We use all our human, technical and IT resources to protect your data. You can equally contribute to the protection of your data as follows:

- install anti-virus software, anti-spyware software, a firewall and keep this software up-to-date;
- do not leave your equipment and mobile devices unattended;
- Immediately notify the Bank if you lose your digipass or if your itsme account has been hacked, so the bank can block your accounts;
- log out of online banking tools when you are not using them;
- keep your passwords strictly confidential, use strong passwords (avoid combinations of letters and numbers that are easy to guess) and make use of two factor authentication.
- stay alert on the internet and learn to recognise suspicious activities, such as website address changes or phishing emails asking for personal data.

9. Changes to this Privacy Statement

We may modify this Privacy Statement to comply with any changes in the law and/or to reflect the way the Bank processes personal data. This version was published on the 1st of November 2025 and will be effective as from the 1st of January 2026. The most recent version can be found on the website www.delen.bank. We will inform you of any significant changes through the usual channels.