Bellatrix Asset Management S.A.

Privacy policy

Date of review: June 2025

BELLATRIX
ASSET MANAGEMENT

Table of contents

Document control:

Version	Date	Description	Created/reviewed by	Approved by the Board
1	30/10/2020	Creation of procedure	Bellatrix Asset Management S.A.	11/12/2020
2	30/11/2021	Review of procedure	Bellatrix Asset Management S.A.	15/12/2021
3	30/11/2022	Review of procedure	Bellatrix Asset Management S.A.	06/12/2022
4	15/11/2023	Review of procedure	Bellatrix Asset Management S.A.	11/12/2023
5	20/06/2024	Translation and restatement	Phoenix Solutions Luxembourg S.A.	23/09/2024
6	03/06/2025	Review of procedure	Bellatrix Asset Management S.A.	23/10/2025

1) INTRODUCTION

Bellatrix Asset Management S.A. (hereinafter referred to as the "**Company**") attaches particular importance to data protection.

This privacy policy (the "**Policy**") is intended for users of the Company's website, customers, direct business relations, service providers and employees of the Company (also collectively hereinafter referred to as the "**data subject(s)**").

As controller of the collection and processing of your personal data, the Company is responsible for the use of your personal data in the context of the Company's activities. The Company only uses this data in the context of its activities. The purpose of this Policy is to inform you about the processing of your data, its protection and your rights with regard to your data.

2) PROTECTION OF PERSONAL DATA

The Company collects your personal data:

- **Directly** (for example, when you contact us) or;
- **Indirectly** (for example, when one of your employees comes into contact with the Company).

Personal data may only be collected and processed in accordance with the rules relating to data protection laws.

2.1 When is personal data collected?

The personal data of website users, customers, direct business relations, service providers and employees may be collected during:

- Browsing the Company's website;
- The user contacting the Company using the form available in the "Contact" tab on the website;
- Subscription to information feeds such as newsletters;
- When recruiting a new employee for the Company;
- When carrying out a contract for the supply of goods and services on behalf of the Company;
- Face-to-face meetings for service requests.

2.2 The purposes of collecting personal data

The personal data collected from users of the Company's website is processed for the following purposes:

- To provide services or information requested by a user via the website, a direct business relationship or a customer;
- To keep a follow up of the employee's progress within the Company and compensate him/her with a remuneration;

- To ensure the security of personal data against external intrusion attempts or other computer attacks;
- To carry out statistical analyses of visitor numbers in order to develop the services offered by the Company as effectively as possible.

If data is processed for a purpose other than that stated at the time of collection, the data controller is required to inform the data subject directly, stating the other purpose and any other relevant information.

2.3 Data processing conditions

The processing of personal data must comply with the law and be lawful. The processing of such data by the Company is lawful only under the following conditions:

- The data subject has consented to the processing of his/her personal data for one or more specific purposes.
- The processing is necessary for the performance of a contract to which the data subject is party or for the performance of pre-contractual measures taken at the data subject's request.
- The processing is necessary to comply with a clear and precise legal obligation to which the Data Controller is subject.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller.

If the data subject has given his/her consent to the processing of his personal data, the Data Controller must be able to demonstrate this consent at any time.

In this context, the "Data Controller" is "*the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing operation; where the purposes and means of such processing are determined by Union law or by the law of a Member State, the controller may be designated or specific criteria for such designation may be laid down in Union law or in the law of a Member State*".

2.4 The consequences of not providing personal data

Some of the personal data to be provided by the data subject is compulsory, while other data is optional. If the data subject does not wish to provide essential data, this may result in the requested service or information not being provided.

The data subject will always be informed of the compulsory or optional nature of any information when data is collected.

2.5 The data collected

The Company collects and uses personal data in the context of its regulatory obligations and the work we offer. In this context, we collect the following data from the Company's directors, employees and clients:

- Personal identification data (name, address, telephone number);
- Identification data issued by public services (identity card and passport numbers);
- Personal details (date and place of birth, nationality);
- Electronic identification data (email address, electronic signature);
- Data relating to education, training and qualifications (level of education, professional qualifications);
- Data relating to occupation and employment (job, name of employer, remuneration);
- Bank details.

The following personal data may be collected via the Company's website:

- Basic identification data (surname, first name, e-mail address or telephone number);
- Technical connection data (your computer's IP address, date and time of connection, cookies, saved preferences and pages visited);
- Geolocation data.

3) SHARING PERSONAL DATA

As part of our work, and in order to carry out our missions, your personal data may be shared with the following persons:

- Service providers/suppliers performing services on our behalf;
- Supervisory, financial, tax, judicial, administrative authorities or state agencies, public bodies, at their request and within the limits authorised by the laws and regulations;
- Certain regulated professions such as lawyers, notaries and auditors.

4) OUR INTERNAL POLICY ON YOUR PERSONAL DATA

The Company's employees will ensure that information concerning the Company, its customers and its other stakeholders (counterparties, subcontractors, shareholders, directors, etc.) is kept confidential. Internally, they will respect the "need to know" principle and the "Chinese walls" set up between independent functions.

To this end, employees strictly observe the duty of confidentiality and discretion towards customers.

They shall ensure that, except where required or authorised by law, they do not disclose to a third party any information gathered about the customer or the customer's transactions. They shall carefully manage customer information in order to prevent any inappropriate disclosure of such information,

including within the institution itself. They shall not exploit or use customer information for purposes other than those for which it was communicated to them, in compliance with the rules on the protection of personal data, including the principles of transparency and customer access to data concerning them.

4.1 Data likely to contain personal information

The data we use relating to your financial situation, your investments and your personal objectives will be treated with the same duty of discretion. Compliance with the duty of discretion and professional secrecy means that measures are taken to protect your personal information, ensuring its confidentiality and security at all times.

This protection takes various forms, including:

- We undertake to discuss the files only with persons who need the information in the normal course of their activities within the Company;
- We undertake to systematically tidy up the files handled and not to leave them in view and/or lock up confidential documents (“clean desk policy”);
- We undertake to ensure that documents are not left on printers, photocopiers, etc.;
- We undertake to protect confidential files with passwords;
- We undertake to allow access to confidential files and information only to the dedicated functions (i.e. compliance function), as detailed in the IT Procedure of the Company;
- We undertake to ensure the confidentiality of meetings/discussions (closed meeting rooms, no discussions in public places and particularly on public transport);
- We are committed to providing maximum protection for our IT equipment, by installing firewalls and antivirus software, and by protecting our computers with VPN connections and session codes.

4.2 Insider information

The Company employees will pay particular attention to inside information concerning companies or financial instruments listed on a regulated or unregulated market. Inside information is defined as:

- Information not made public (communication, press, etc.);
- Information that is specific (concrete);
- Information made public that is likely to influence the price of the company or the financial instrument or a related instrument.

When employees have access to inside information, they must refrain from disclosing this information outside the normal course of their duties. Otherwise, they would be committing insider trading, which is punishable under criminal law.

Employees who leave the Company are required to respect the confidential or privileged nature of any information to which they have had access, even after they have left the Company, without any time limit.

5) OUTSOURCING

The Company may have recourse to external delegates for specific functions or tasks. In particular, the Company outsources the UCI administration role for its funds (UCITS) under management. In that context, the Company is keen to ensure that:

- Its delegates (the "**Data Processor(s)**") comply with all relevant requirements;
- An initial due diligence is conducted before entering into any agreement with any party, evaluating their expertise, reliability and resources to implement technical and organizational measures, as well as ensuring processing security in compliance with Luxembourg Data Protection Regulations;
- The service level agreements entered into by and between the Company and its Data Processors incorporate minimum standards aligned with Luxembourg Data Protection Regulations.

Furthermore, as part of its ingoing monitoring, the Company ensures that its Data Processors consistently adhere to Luxembourg Data Protection Regulations, including the lawfulness of data processing, legitimacy of data transfers, transparency towards data subjects, management of data retention period and processing security.

6) TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA (EEA)

The Company does not transfer your data outside the EEA.

If your data is to be transferred outside the EEA, the transfer will take place on the basis of a decision issued by the European Commission, having recognised the country to which the data will be transferred as having an equivalent level of protection to those in the EEA.

In the event of a transfer to a third country, we will put in place contractual clauses approved by the European Commission to ensure the protection of your data.

7) RETENTION OF PERSONAL DATA

In view of our regulatory obligations, your personal data is kept for a period of 5 years from the end of the business relationship.

Electronically archived data is stored on the Company's server in Luxembourg and on the back-up server in Luxembourg for a period of 5 years from the end of the business relationship.

8) DATA BREACH

A personal data breach is defined as any security incident, whether malicious or not and whether intentional or not, which has the effect of compromising the integrity, confidentiality or availability of personal data (e.g. the loss of an unsecured USB key containing a copy of a company's customer database, or information about the company).

The detection of a personal data breach incident should lead the organisation to focus its efforts on resolving it by adopting any appropriate measures to remedy any breach and limit its consequences for the people whose data is affected. However, these measures should not obscure the need for the organisation to assess at the same time whether or not it should notify the CNPD of the incident.

The obligation to notify carries heavy penalties in the event of failure to comply. The RGPD sets a very strict deadline for notification: 72 hours at the latest after becoming aware of the incident.

In order to be as proactive as possible, the Company has a register for monitoring data breaches (whether or not declared to the CNPD) and a data breach declaration form.

9) COOKIES POLICY

The Company's website uses cookies to improve user experience and site performance. Among other things, cookies make it possible to personalise the home pages by saving the preferences that a user may express during a subsequent visit. These cookies can also be used to secure access or to identify the sections that have been visited or to track changes in preferences.

Users give their consent, which must be prior, free and explicit, to cookies that they authorise to be activated and that collect data about them. This consent to cookies must be granular in order to comply with the General Data Protection Regulation (EU Regulation 2016/679) and the guidelines on cookies and other tracers issued by the Luxembourg National Data Protection Commission (CNPD). A user must be able to choose certain cookies and not accept them all or reject them all simultaneously.

The Company uses cookies on its website for the following purposes:

8.1 Strictly necessary cookies (consent not required)

These cookies enable essential functions to be activated. A website cannot function without strictly necessary cookies. Any user who refuses the use of these cookies is asked to leave the site and abandon their browsing session immediately.

The Company's website uses essential cookies for the following purposes:

- **Registration of the user's choice concerning cookies**; these cookies must be accepted in order for the user's browsing on the website to be completed.
- **Recording of responses to a contact form**; after accepting the essential cookies, the user can contact the Company via its form available in the "Contact us" tab.
- **Service customisation**; these cookies enable users to customise their browsing on the Company's website, for example by changing their language preference.
- **Security**: essential cookies ensure greater security on a website.

This category includes cookies which enable the Company to comply with legal obligations to ensure a safe online environment.

Users are made aware of the existence of these cookies when they first connect to the Company's website via the cookies banner.

8.2 Functional cookies (consent required)

These cookies placed on a website must be approved by the user in order for them to be functional when browsing the Company's website. The user must have the choice of accepting all of them or approving only a selection. If the user refuses one of these cookies, the cookie(s) cannot be activated during the user's browsing session.

The functional cookies found on the Company's website are used for the following purposes:

- **Profiling**: cookies used to create a personalised profile for a user when personal data is collected.
- **Tracking**: cookies make it possible to identify and follow a user's browsing on a website. They can also be used to find out how long a user remains connected to the site as a whole or to a particular session.
- **Geolocation**: cookies that simply allow the user to be geolocated in order to obtain additional information.

8.3 Refusal and withdrawal of consent

The user must have the full choice of accepting or refusing cookies when connecting to the Company's website for the first time.

However, if users change their mind, they can do so at any time, and they must also be able to change their choice easily by means of a direct link to the various cookie settings (via the cookies banner).

8.4 Period of validity and renewal of a user's consent

Consent for these cookies is retained for 12 months, in accordance with the recommendations of the CNPD. A request for renewal of consent will be requested again after this 12-month period. The personal data collected by cookies is kept for 12 months.

However, if a user changes terminal or deletes the history of these cookies, consent to the various cookies will be requested again the next time the user connects to the BAM website without waiting for the period of validity to expire.

The Company's website must also ask for the user's consent again before the end of the validity period, for example when:

- The data collected via cookies has been modified;
- The purpose of data processing is modified.

10) YOUR RIGHTS

In accordance with the EU Data Protection Regulation 2016/679 and taking into account the regulatory obligations to which we are subject, you have the right to exercise the following rights:

- Right of access (Article15.);
- Right of rectification (Article 16.);
- Right to erasure / right to be forgotten (Article17.);
- Right to restrict processing (Article 18);
- Right to data portability (Article20.);
- Right to object (article 21.).

If you wish to exercise your rights, you can send us a letter or e-mail to the addresses given in point IX.

Where you expressly make any request concerning your personal data, the data controller must provide as soon as possible, which is one month from receipt of the request, all the measures taken following the formulation of this request by yourself.

The Company undertakes to facilitate the exercise of your rights. Under no circumstances shall the Company refuse to comply with a request, unless it is unable to identify the person concerned.

The response time may be extended by two months if the request is complex or if the Company receives a large number of requests. This extension must be notified to you within one month of receipt of the request, stating the reasons for the extension.

If the Company does not take any action on a request, the Company must inform you without delay and at the latest within one month of receipt of the request, stating the reasons for its inactivity and the possibility of lodging a complaint with a supervisory authority and of taking legal action.

No payment will be required from the Company to provide the information, to carry out any communication and to take all necessary measures. However, when requests are manifestly unfounded or excessive due to their repetitive nature, the Company may:

- To require the payment of “reasonable” fees, taking into account the administrative costs that may be incurred in order to provide the information, make the communications or take the necessary measures requested;
- Refuse to comply with these requests.

The Company must be able to demonstrate that the claim is manifestly unfounded or excessive.

In order to process your request as efficiently as possible and to ensure that your personal data is not passed on to any malicious person, we would be grateful if you could include a copy of your identity document (in paper or PDF format) to enable us to identify you.

11) CONTACT

If you have any questions about the processing of your personal data, or if you wish to exercise your rights, you can contact us at:

By telephone: +352 26 25 66 20

By email to : info@bellatrix.lu

By post: **Bellatrix Asset Management**
31 boulevard prince Henri
L-1724 Luxembourg