Falcore

Privacy Statement

- We process personal data only where we have a lawful basis and a defined purpose.
- We use personal data to onboard and serve clients, execute transactions, meet legal obligations, maintain safe and sound operations, arrange meetings and events between investors and corporate representatives (corporate access events), and improve our services.
- We may share data with our branches, subsidiaries, shareholders, regulators, market infrastructures and trusted service providers where necessary and lawful.
- Van Lanschot Kempen N.V. (“VLK”) provides significant outsourced technology and operational support to the Controller. We remain accountable for the processing carried out on our behalf.
- You can exercise your privacy rights and lodge a complaint with the competent data protection authority.

Falcore B.V. | Amsterdam, 14 December 2026

Your privacy is important to us

Falcore B.V. ("Falcore", "we", "us" or "our") respects your privacy and handles personal data responsibly and carefully. This Privacy Statement explains which personal data we process, why we process it, with whom we may share it, how long we keep it and which rights you have.

Falcore is a Dutch investment firm with its head office in Amsterdam, and a Belgian branch. Falcore provides services to professional clients, elective professional clients and eligible counterparties. Its activities include equities research, equities sales, equities trading, corporate access and equity capital markets services.

For the processing described in this statement, Falcore generally acts as Data Controller ("Data Controller" or "Controller"). Where another entity independently determines why and how personal data is processed, that entity may act as separate controller. Where a service provider processes data only on our instructions, it acts as our Processor.

1. When do we update this Privacy Statement?

We will update this Privacy Statement when our services, organization, systems, legal obligations or ways of processing personal data change. We will publish the current version through our website and, where appropriate, inform affected individuals of material changes.

2. What is personal data and what is processing?

Personal data is any information relating to an identified or identifiable natural person. Processing includes collecting, recording, organizing, using, viewing, sharing, storing, restricting, deleting or otherwise handling personal data.

3. Which types of personal data do we process?

Category	Examples
Identification and contact data	Name, address, business contact details, signature, date and place of birth, nationality and identification document details.
Professional and relationship data	Employer, role, authority, directorships, business relationships, client classification, mandates and powers of attorney.
Financial and transaction data	Bank account details, holdings, orders, trades, settlement information, transaction history, source-of-funds/wealth information where required.

Category	Examples
Compliance and integrity data	Client due diligence information, beneficial ownership, sanctions/PEP screening results, adverse media, fraud indicators and information relevant to market abuse controls.
Communications and interaction data	Emails, correspondence, meeting notes, complaints, call recordings and electronic communications where recording is required or permitted.
Digital and technical data	IP address, device identifiers, log data, authentication data, website usage and cookie data.
Corporate access and event data	Registration details, dietary or accessibility information voluntarily provided, attendance, meeting preferences and event communications.
Special-category and criminal-offence data	This category of data is only processed where strictly necessary and legally permitted, for example when the information is requested to perform due diligence activities, with the aim of complying with AML/CFT requirements. It is also possible that this kind of data are received via communications directly from the clients, with the aim of performing the KYC screening process or accessibility information provided for events.

4. From where do we obtain personal data?

We obtain personal data directly from you or from the organization you represent.
We may also obtain data from:

- VLK and KBC Securities in connection with the transfer of existing client relationships to Falcore;
- Public registers and sources, such as company, beneficial ownership, insolvency and sanctions registers;
- Screening and information providers for client due diligence, sanctions, PEP and adverse-media checks;
- Trading venues, market infrastructures, banks, brokers, counterparties and other market participants in connection with transactions and investment services; and
- Regulators, public authorities and professional advisers where lawful and relevant to our services or obligations.

Where your personal data has been transferred to Falcore B.V. in connection with the transition of existing client relationships or business activities, you will also have received separate information about that transfer from Van Lanschot Kempen or KBC Securities.

5. Why and on what basis do we process your personal data?

We process personal data for the purposes below. The applicable lawful basis depends on the activity and the circumstances.

Purpose	What this involves	Lawful basis
Client acceptance and ongoing due diligence	To identify and verify clients and connected persons, assess integrity risks, screen sanctions and PEPs, determine client classification and maintain due diligence files.	We process your personal data to comply with a legal obligation, legal requirements and public orders: in this case the identification, verification and assessment of the clients is necessary to comply with applicable financial regulatory, anti-money laundering laws or sanctions requirements. In some cases, we process your personal data based on our legitimate interests, which has been duly assessed and

Purpose	What this involves	Lawful basis
		documented to ensure this is appropriate and does not override your rights and freedoms. This happens when additional due diligence is necessary to assess and manage integrity, fraud or business risks. We continually ensure that the impact on your privacy is kept to a minimum and that, in all events, the Controller's legitimate interests remain proportionate to the impact that has on your privacy.
Providing investment and ancillary services	To manage client relationships, distribute research, receive/transmit/execute orders, facilitate trades, provide liquidity, support ECM transactions, settle and report transactions.	We process your personal data for the performance of the contract you entered into with the Controller. The processing is necessary in order to correctly carry out all the necessary activities to provide investment and ancillary services. Additionally, as an investment firm we are obliged to comply with specific laws and legal requirements applicable in financial and banking sectors. In this case, the processing is necessary to comply with reporting requirements. In some cases, we process your personal data based on our legitimate interests, which has been duly assessed and documented to ensure this is appropriate and does not override your rights and freedoms. In this case the processing is necessary to maintain and manage the relationship with an organization represented by the individual concerned. We continually ensure that the impact on your privacy is kept to a minimum and that, in all events, the Controller's legitimate interests remain proportionate to the impact that has on your privacy.
(Corporate access) and events for which you registered or requested to participate.	To organize road shows, conferences, seminars, meetings and related communications. The organization of these events is limited to the audience of clients who have registered for participation.	We process your personal data for the performance of the contract you entered into with the Controller. The processing is necessary in order to provide the services and communications you requested. Subject to your specific Consent, we will use your personal data, such as your name, email address and phone number, to keep you informed about future corporate access events, similar to the ones for which you registered (Corporate Access Events). If you wish to receive this kind of communications, you may provide your specific consent (opt-in), which you can withdraw at any time, following the same process to provide it. In some cases, we process your personal data based on our legitimate interests, which has been duly assessed and documented to ensure this is appropriate and does not override your rights and freedoms. This happens when we send you surveys or feedback requests to improve the quality of the meetings and events in which you participated, and to maintain an efficient business relationship. We continually ensure that the impact on your privacy is kept to a minimum and that, in all events, the Controller's legitimate interests remain proportionate to the impact that has on your privacy.
Communication recording and monitoring	To record and retain telephone and electronic communications, supervise conduct, evidence instructions, resolve disputes, and support training and quality.	We process your personal data to comply with legal obligations, legal requirements and public orders: in this case, communication must be recorded, monitored or retained to comply with applicable financial services laws. In some cases, we process your personal data based on our legitimate interests, which has been duly assessed and documented to ensure this is appropriate and does not override

Purpose	What this involves	Lawful basis
		your rights and freedoms. This happens when record keeping is necessary to evidence instructions and improving service quality. We continually ensure that the impact on your privacy is kept to a minimum and that, in all events, the Controller's legitimate interests remain proportionate to the impact that has on your privacy.
Regulatory reporting and cooperation	To report transactions, respond to competent authorities, cooperate with investigations and comply with information, record-keeping and market-integrity obligations.	We process your personal data to comply with a legal obligation, legal requirements and public orders: in this case the processing is required for regulatory reporting, record keeping or cooperation with competent supervisory authorities. We, as an investment firm, are legally required to use all means to prevent, detect and report suspicious activities (such as money-laundering and terrorist financing) to supervisory authorities. This is a matter of considerable public interest. The Controller is required to take the necessary steps to this end, at both centralized and local levels
Security, resilience and fraud prevention	To protect systems, premises, clients, markets and staff, detect incidents, prevent fraud and maintain sound business operations.	We process your personal data to comply with a legal obligation, legal requirements and public orders: in this case, the processing is required under applicable security, resilience and financial regulatory requirements. In some cases, we process your personal data based on our legitimate interests, which has been duly assessed and documented to ensure this is appropriate and does not override your rights and freedoms. In this case we process the necessary information to protect our systems, operations, premises, clients, staff and markets, and to prevent and detect fraud and security incidents. We continually ensure that the impact on your privacy is kept to a minimum and that, in all events, the Controller's legitimate interests remain proportionate to the impact that has on your privacy.
Marketing and relationship management	To send relevant services, research, events or business-development communications and manage preferences.	Subject to your Consent, we will use your personal data, such as your name, email address and phone number, to suggest and recommend our financial services, products and business development communications (Marketing Communications). If you wish to receive this kind of communications, you may provide your specific consent (opt-in), which you can withdraw at any time, following the same process to provide it. Likewise, we will use your personal data, such as your name, email address and phone number, to invite you to dedicated events which may interest you (Events Planning). If you wish to receive this kind of communications, you may provide your specific consent (opt-in), which you can withdraw at any time, following the same process to provide it. In some cases, we process your personal data based on our legitimate interests, which has been duly assessed and documented to ensure this is appropriate and does not override your rights and freedoms. We will only use your email address to keep you informed about services or products necessary to maintain fruitful our business relationship(s) and communicate relevant development(s), research or events (Soft Spam). You can still opt out from this service by objecting to the processing of your data for this purpose.

Purpose	What this involves	Lawful basis
Analytics and service improvement	To analyze service use, improve products, controls and client experience, and produce management information, using aggregated or anonymized data.	In some cases, we process your personal data based on our legitimate interests, which has been duly assessed and documented to ensure this is appropriate and does not override your rights and freedoms. In this case, we will use analytics to understand the use of our services, improve products, controls and client experience, and produce management information. We continually ensure that the impact on your privacy is kept to a minimum and that, in all events, the Controller's legitimate interests remain proportionate to the impact that has on your privacy.
Legal claims and corporate transactions	To establish, exercise or defend legal claims and support audits, reorganizations, transfers or transactions involving the business.	We process your personal data to comply with a legal obligation, legal requirements and public orders: in this case, the processing is necessary in order to allow us to exercise or defend legal claims and comply with supervisory authorities' orders. In some cases, we process your personal data based on our legitimate interests, which has been duly assessed and documented to ensure this is appropriate and does not override your rights and freedoms. In this case, the processing is required for internal and regulatory reporting and internal control, and to defend rights and communicate as a company. We continually ensure that the impact on your privacy is kept to a minimum and that, in all events, the Controller's legitimate interests remain proportionate to the impact that has on your privacy.

Legitimate interests

Where we use legitimate interest as a lawful basis for processing your personal data, we have assessed and duly documented the appropriateness, the necessity and the proportionality of our interests to make sure that your rights and freedoms are not overridden or harmed in any way.

Legitimate interests is used only in those cases where the purposes (listed above) cannot be achieved using alternative means.

You always have the right to request additional information regarding the processing of your data based on this lawful basis, by contacting us using the Contact details available in Section 14.

You have the right to object at any time to any processing based on legitimate Interest, according to your particular situation, by contacting us using the Contact details available in Section 14. Upon receipt of the request, we will no longer process the personal data, although in some cases, we can refuse the objection and continue the processing by demonstrating compelling legitimate grounds for the processing which override your interests, rights and freedoms.

6. Automated individual decision-making, including profiling

Falcore uses automated tools only where strictly necessary for the nature of the services provided to you, such as to support screening, monitoring, risk detection and workflow decisions. These tools support decision-making but are not intended to produce legal or similarly significant effects solely by automated means without appropriate human involvement.

Whenever automated decision-making does take place, we make sure that the processing of your personal data is performed appropriately and transparently. We will communicate all the necessary information to you, including a description of the fully automated decision, an explanation of the underlying argumentation and what the consequences are. We also ensure that all the steps of the processing are lawful, and that suitable safeguards are in place, including at least the right to obtain human intervention from the Data Controller, to express your point of view, and to contest the decision.

7. With whom may we share personal data?

We share personal data with third party recipients only where this is necessary, proportionate and lawful. Third party recipients remain accountable for processing of personal data for their own purposes. Third party recipients may include:

- a subsidiary entity of the Controller based in Belgium Falcore BV, Belgian Branch;
- Van Lanschot Kempen and KBC Securities, where necessary for the transition of contributed business, shareholder services, client coverage, integrity controls or other defined arrangements;
- banks, brokers, trading venues, settlement agents, clearing organizations, issuers, syndicate members, research distribution platforms and other market participants;
- courts, law-enforcement bodies, tax authorities, the AFM, DNB, AP, NBB, FSMA, FIUs and other competent authorities, where required or permitted by law.
- Where a Processor processes personal data on our behalf, we require appropriate contractual, confidentiality, security, audit and sub-processing safeguards. Falcore remains accountable for processing performed on our behalf. The following categories of Processors are in scope:
- Van Lanschot Kempen shall act as Data Processor, as a provider of outsourced IT, operational, HR, finance, procurement, internal control, risk/compliance support, client administration/monitoring and communications services;
- professional advisers, auditors, insurers, screening providers, cloud/technology providers and other Processors that support business processes and continuity.

You may request the full list of third parties by using the Contact details available in Section 14.

8. Transfers outside the European Union (EU) and the European Economic Area (EEA)

We process your personal data within the European Union and European Economic Area. However, when we collaborate with a third party, personal data may be accessed from or transferred to the countries where the third-party data centers are located; this means that some of your data is processed in countries outside the EEA.

Where this occurs, we make sure that an applicable transfer mechanism and appropriate safeguards are in place in accordance with the GDPR and other relevant data protection laws.

By preference, the transfer happens towards Countries which are deemed to offer the same level of data protection as in EU and EEA member states, and which have been granted with an adequacy decision issued by the European Commission. Depending on the circumstances, the transfer may occur towards Countries viewed by the European Commission as not offering an adequate level of protection; in these cases, the Controller can cover the deficiency by relying on different appropriate safeguards such as agreeing the required contractual guarantees with those third parties (such as standard contractual clauses, approved by the European Commission), providing control mechanisms, and implementing technical and organizational measures.

9. How do we protect personal data?

We use technical and organizational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

Only persons with appropriate authorization can access your personal data, and then only if that data is relevant to the performance of their duties. In principle, your personal data will only be processed and consulted by certain departments:

- departments with which you now have, have previously had or would in future like to have a contractual relationship;
- departments which need to be involved in the provision or aftercare of services;
- departments which fulfil legal requirements or requirements imposed by regulators, or stemming from corporate governance principles;
- departments that are tasked with preventing fraud, including money laundering, by staff and customers.

Persons who are authorized to consult your data are moreover bound by a strict professional duty of confidentiality and must abide by all technical requirements to ensure the confidentiality of your personal data and the security of the systems in which the data are held.

10. How do we handle personal data breaches?

A personal data breach is a security breach that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. We assess and document suspected breaches and notify the competent data protection authority where required. We inform affected individuals where the law requires this because the breach is likely to result in a high risk to their rights and freedoms.

If you are aware of a breach or if you believe that your data have been breached in any way, you may refer this to the Controller by using the Contact details available in Section 14.

11. How long do we keep personal data?

We keep personal data no longer than necessary for the relevant purpose and in accordance with applicable legal and regulatory requirements. Retention periods vary by data category and activity: for processing related to the performance of contracts, we retain your data for 10 years after the end of the said contract or the execution of a transaction. For commercial claims, we retain the data for up to 30 years after the end of the business relationship.

In determining the applicable period, we consider the purpose and nature of the processing, the duration of the client or business relationship, applicable legal and regulatory retention requirements, relevant limitation periods and the need to establish, exercise or defend legal claims. For example, separate periods apply to client due diligence records, transaction records, recorded communications, complaints and event data.

We may retain data longer where this is necessary for legal proceedings, regulatory investigations, risk management, evidence or the protection of legal rights. When retention is no longer justified, data is securely deleted or anonymized.

12. What rights do you have?

Subject to the conditions, exceptions and restrictions set out in applicable data protection law, you may exercise the following rights::

Right	What it means
Access	You can ask whether we use your personal data. If we do, you can ask us what personal data we use, why we use it, where it came from, who we share it with and how long we keep it. You can also ask for a copy of your personal data.
Correct your personal data	You can ask us to correct personal data that is inaccurate. You can also ask us to complete personal data that is incomplete.
Delete your personal data	You can ask us to delete your personal data. We will do this when there is no longer a valid reason to keep it. We may need to keep some data, for example because the law requires this.
Restrict the use of your personal data	You can ask us to stop using some of your personal data for a period of time. For example, you can do this while we check whether the data is correct. We may still store the data during this period.
Object to the use of your personal data	In some situations, you can ask us to stop using your personal data. This applies, for example, when we use the data because it is in our legitimate interests. For example, you may always object to the use of personal data for direct marketing purposes.
Receive or transfer your personal data	In some situations, you can ask us to provide personal data that you gave us in a digital format that is easy for another organization to use. You can also ask us to send the data directly to another organization when this is technically possible.
Withdraw your consent	If we use your personal data because you gave us permission, you can withdraw that permission at any time. After this, we will stop using the data for that purpose unless we have another obligation or legal reason to continue.
Ask for a person to review an automated decision	In some situations, you have the right not to be subject to an important decision made solely through automated processing, without human assessment. You can ask a person to review the decision, explain your situation and challenge the decision.

We may need to verify your identity and may refuse or limit a request where the law permits or requires us to do so, including to protect the rights of others, comply with record-retention duties or preserve legal privilege. We normally handle requests free of charge, but may charge a reasonable fee or refuse to act on manifestly unfounded or excessive requests where permitted by law.

13. Cookies and website tracking

If our website uses cookies or similar technologies, the separate Cookie Statement will explain which technologies are used, their purposes, retention periods, recipients and how you can manage your preferences. Non-essential cookies will be used only where the required consent has been obtained.

14. Questions, requests and complaints

For privacy questions or to exercise your rights, contact:

- Privacy contact: privacyofficerfalcore@falcore-equities.com
- Data Protection Officer: privacyofficerfalcore@falcore-equities.com
- Postal address: Falcore B.V., Amstelplein 2, 1096 BC Amsterdam, The Netherlands

You also have the right to lodge a complaint with the competent data protection authority. In the Netherlands, this is the Autoriteit Persoonsgegevens. Depending on where you are located and the processing concerned, another EEA supervisory authority may also be competent.

15. Controller details

Item	Details
Legal entity	Falcore B.V.
Registered office	Amsterdam, the Netherlands
Chamber of Commerce	99663503
Belgian branch	Falcore BV, Belgian Branch, Kievit Toren, Van Immerseelstraat 66, 2018 Antwerp, Belgium
Website	www.falcore-equities.com
General contact	info@falcore-equities.com

Falcore B.V.
Amstelplein 2 17th Floor
1096 BC Amsterdam
The Netherlands