

General Privacy Notice

1 General Information

This privacy notice (the “**Privacy Notice**”) explains how **InvesTRe S.A.** and **Moniflo** (together “**InvesTRe S.A.**”; “**we**”, “**us**” or “**our**”) collect, use, process, share and protect personal data in the course of its business activities and the provision of its services.

For the purposes of this **Privacy Notice**, “personal data” means any information relating to an identified or identifiable natural person, whether directly or indirectly, regardless of its form or medium. This may include, for example, names, contact details, identification numbers, financial information and any other data that can be linked to an individual.

We process personal data in accordance with the EU General Data Protection Regulation (Regulation (EU) 2016/679) (the “**GDPR**”), applicable national data protection laws, including the Luxembourg law of 1 August 2018, and relevant regulatory guidance, including that of the European Data Protection Board (collectively, the “**Data Protection Laws**”).

Depending on the circumstances, we may act either as a data controller or a data processor. In all cases, we are committed to ensuring that personal data is processed lawfully, fairly and transparently, and that appropriate technical and organisational measures are implemented to protect such data against unauthorised access, loss, misuse or unlawful processing.

This **Privacy Notice** describes:

- how and why we collect personal data,
- how we use and share it,
- how long we retain it,
- the safeguards we apply, and
- your rights under the Data Protection Laws and how to exercise them.

By using our services or interacting with us, you acknowledge that your personal data may be processed as described in this **Privacy Notice**. If you have any questions or wish to exercise your rights, please contact us using the details provided in the “Contact Us” section below.

1.1 InvesTRe S.A. as a data controller

Except as further described below, InvesTRe S.A. is to be considered the data controller with respect to your personal data processing.

InvesTRe S.A., acting as a data controller, is committed to protecting your privacy and ensuring the security of your personal data. As a data controller, we are responsible for determining “how” and “why” your personal data is processed, in accordance with the

requirements of GDPR. This means we are responsible for collecting, processing, and safeguarding your personal data. Our role as a data controller entails ensuring that your personal data is processed lawfully, fairly, and transparently. We take your privacy seriously and aim to be transparent about our data processing activities.

2 Data controller details

- Data Controller: InvesTRe S.A.
- Address: 209 Rue des Romains, Bertrange, L-8041, Luxembourg
- Registered Information: InvesTRe S.A. is registered with the commercial register under B249656.
- Representative: Georges Bock, CEO
- We have appointed a data protection officer who advises and guides us on matters related to the implementation and maintenance of our data protection management system. You can contact our data protection officer at: privacy@investre.eu

2.1 InvesTRe S.A. as a data processor

Depending on our professional mandate, InvesTRe S.A. may also act as a data processor under specific circumstances. We (as a data processor) will solely determine when such a situation occurs and will inform you (as a data controller) accordingly. This section defines the conditions under which we undertake to process personal data on your behalf as a data processor.

In this regard, we process personal data as necessary for us to perform our mission. To this end, we will rely on your instructions with regards to:

- The nature of the operations to be carried out;
- The purpose of the processing;
- The data processed;
- The categories of data subjects concerned by the data processing.

About our obligations towards you, we undertake to:

- Process the data for the sole purpose for which you have transmitted it to us and in accordance with your documented instructions;
- Apply the principles of data protection by design and data protection by default with respect to any activity by virtue of which we process data;

- Assist you with sufficient guarantees by appropriate technical and organizational measures to ensure that the processing complies with the requirements of these regulations and guarantees the protection of the data subjects' rights;
- Guarantee the security, confidentiality and integrity of the personal data processed;
- Provide the necessary awareness and training to persons authorized to process personal data on data protection;
- Inform you in the event that we consider that such processing may involve a breach of applicable law, as well as when there is a risk affecting your personal data or their processing;
- In accordance with your request, delete or return to you all that personal data (in case we process such personal data only in our capacity as processor), and delete existing copies of any such personal information, except it is mandatory for us to retain that personal data;
- Provide you all information necessary to demonstrate compliance with the obligations set out in the GDPR and allow for and contribute to audits, including inspections, conducted by you (as a controller) or another auditor mandated by you.

Whenever possible, we (as data processor) will assist you (as data controller) in fulfilling your obligations to comply with requests to exercise the rights of any individuals concerned by the processing at hand, including the right of access, rectification, erasure, and objection; the right to restriction of processing; the right to data portability; and the right not to be subject to an automated individual decision.

In case of using sub-contractors or replacing them, to carry out specific processing activities in order to perform our mission, we will notify you and will act with professional diligence.

This specific section is without prejudice to other non-contradictory provisions of this **Privacy Notice** and our commitments to respect and promote data protection principles.

3 What kind of data we process

To provide our services, we need to collect and process information about you. The data we collect depends on the context of your interactions with InvesTRe S.A and the choices you make including the services which are provided to you.

You can choose what data you allow us / or not to collect. Should you refuse to share your data, we may not be able to provide our service to you.

The data we collect/we may collect, and process include the following:

- **Identification data:** we collect data about you such as your first and last name, email address, postal address, phone number and other similar contact details, date and

place of birth, gender, country, preferred language and, where you interact with our websites or online forms, identifiers such as your IP address and any contact details you voluntarily provide (e.g. for referral campaigns or to receive marketing communications).

- **Electronic identification data:** we use cookies and similar technologies to collect data on how you use our website and interact with our marketing communications. This may include, for example, your IP address, device and browser information, browsing activities, which pages you have visited, how long you stayed on them, which items you clicked on, and general usage patterns. Some of this information is strictly necessary to operate the website, while other data is optional and can be configured through your cookie settings. **Please refer to our dedicated [Cookie Notice](#) for further details.**
- **Business contact information:** we collect data about you such as job function, job title, department, organisation name, company size and location, business contact details, and whether or not you are acting on behalf of a client or counterparty.
- **Financial information:** we collect your financial information, such as bank account details, billing or payment information, where necessary to process payments, fulfil contractual obligations, or for related accounting, legal or regulatory purposes.
- **Contractual information:** any information provided by the data subject or generated in the context of our relationship that allows InvesTRe S.A. to enter into, perform, manage or evidence its contractual duties and services, including correspondence, requests, forms, feedback, survey responses and other communications necessary to address your inquiries or improve our services.
- **Sensitive personal data** such as CV and/or Criminal Record. Such data is processed strictly to the limited extent necessary for InvesTRe S.A. in the context of employment, the performance of a contract with a client, or to comply with a legal or regulatory obligation, and is subject to enhanced safeguard

4 How we process data

By interacting with us, directly or indirectly, you accept that we process your personal data.

InvesTRe S.A will collect and process your personal data, when:

- you visit our firm website, use our applications and/or visit social media pages;
- you show interest in or may be interested in our firm or in our services;
- you apply for a position within our firm;
- you or your company plan on becoming and/or become(s) our customer or supplier;
- we provide services to you or our clients in general.

Depending on InvesTRe S.A activities, we also may obtain your information from other sources (e.g.: affiliates, business partners or other third-party sources) where they are authorized to share such information with us such as:

- Updated business address information;

- Identification data;
- Financial information;
- Contractual information.

We may also obtain information from trusted third-party verification or compliance providers, public registers or screening databases where necessary to perform identity verification, due diligence, fraud prevention or other regulatory checks.

InvesTRe S.A may use AI technologies to enhance the services provided to our clients. Depending on the specific business activity, client documents may be uploaded into secure AI tools. We have integrated this technology securely and responsibly, establishing specific usage guidelines and training our personnel on effective and safe AI tool use.

Furthermore, our arrangements with these technology providers explicitly prevent them from utilising any of your information for their own purposes—such as improving or training their models—or sharing it with unauthorised parties. Your data remains under our control to ensure that it is only accessed in accordance with strict confidentiality obligations and data protection regulations.

We also maintain a comprehensive internal policy governing the safe and responsible use of artificial intelligence, and our staff receive regular training on best practices and security measures. This policy ensures that everyone in our firm is aware of and complies with the strict guidelines and industry standards necessary to protect your data when using artificial intelligence and other advanced technologies.

5 Purpose for collection, use and processing data

For a processing of personal data to be compliant with the GDPR, a legal basis must be identified prior to its implementation.

We may process your personal data:

- If you consent to the processing;
- to satisfy our legal obligations;
- If it is necessary to carry out our obligations arising from any contracts, we entered with you or to take steps at your request prior to entering a contract with you;
- In the public interest;
- In your vital interests, or
- For our legitimate interests, such as to protect our property, rights, or the safety of InvesTRe S.A, our customers, or others



We may contact you by mail, telephone, fax, video conference, email, or other electronic messaging service to notify you about special events, new features or other information that may be of interest to you in accordance with your interaction with InvesTRe S.A. Where required by applicable law, your prior consent will be obtained before sending you direct marketing and you may object or opt out of receiving marketing messages from InvesTRe S.A.

InvesTRe S.A. does not in any way sell, lease, or rent your information to third parties.

Lawful basis	Categories of Personal Data	Purpose for collection use and processing of data
Contract / pre-contract	Identification data	<p>We process personal data following execution and performance of a contract with the data subject or for requested pre-contractual steps between the latter and Investre:</p> <ol style="list-style-type: none"> 1. Enter into, perform and manage contractual or pre-contractual relationships with customers (including onboarding, service delivery and administration and KYC checks where required); 2. Enforce our General Terms and Agreements; 3. Provide, operate and administer our services, digital platforms and applications, including account setup, transactions, record keeping and service delivery; 4. Establish, exercise or defend legal rights in connection with a contractual relationship; and 5. Handle communications, requests, complaints or operational issues and provide customer service. <p>HR</p> <ol style="list-style-type: none"> 1. General processing of personal data for HR administration purposes; 2. Assess and manage job applications and recruitment processes; and 3. Establish, exercise or defend legal rights in connection with a contractual relationship.
	Business contact information	
	Financial information	
	Contractual information	
	Sensitive data – CVs / Criminal Records – only for HR purposes	
	Identification data	We process personal data where required to comply with applicable laws and regulations, including:

Legal obligation	Electronic identification data	<ol style="list-style-type: none"> 1. Compliance with AML/CFT - KYC due diligence and reporting obligations and EU and national financial sanctions regulations, including the detection, prevention and reporting of suspicious activities in accordance with applicable legal requirements; 2. cooperation with supervisory, governmental or judicial authorities; 3. Preventing, detecting and investigating fraud, market abuse, financial crime and other unlawful conduct related to the provision or use of our regulated services; 4. Network and information security requirements; 5. Accounting, tax and regulatory reporting obligations; and 6. Supporting statutory audit, reviewing and testing internal controls, risk management and governance frameworks.
	Financial information	
	Contractual information	
	HR	
	<ol style="list-style-type: none"> 1. Employment, health and safety or HR compliance requirements; 2. fraud prevention and integrity checks; 3. accounting, tax and regulatory reporting obligations; and 4. network and information security requirements. 	
	Identification data	<p>We process personal data to pursue our legitimate business interests, including:</p> <ol style="list-style-type: none"> 1. Protecting and enforcing our legal rights and interests; 2. Monitoring, maintaining and improving the performance, reliability and user experience of our website, applications and services (including error tracking and service optimisation); 3. Analysing communications and interactions for quality assurance, training and service improvement;
	Electronic identification data	

Legitimate interest	Business contact information	<ol style="list-style-type: none"> 4. Business development, analysis and research; 5. Automating and optimising internal workflows and operational processes; 6. Preventing, detecting and investigating fraud, misuse and security incidents affecting our services, systems or users; 7. Ensuring the security of our premises, systems, networks, employees including access controls and identity verification measures (e.g., multi-factor authentication); 8. Managing and developing our business relationships and operations; and 9. Handling disputes, complaints and internal or external investigations.
	Financial information	
	Contractual information	
Consent	Electronic identification data	<p>Where processing is not based on another legal basis, we rely on your consent to:</p> <ol style="list-style-type: none"> 1. marketing activities: send you marketing, newsletter or event communications relating to our services, activities or partner events; 2. personalise and improve your experience on our website or digital channels, including through analytics and preference-based communications.
	Sensitive data – CVs and Criminal Record	<p>HR</p> <ol style="list-style-type: none"> 1. retain your CV or application details and contact you regarding future employment opportunities. <p style="text-align: center;">***</p> <p>You may withdraw your consent at any time, without affecting the lawfulness of processing carried out prior to withdrawal.</p>

As mentioned above, in limited circumstances, we may process special categories of personal data (within the meaning of Article 9 of the GDPR), such as health data, information relating to criminal records or other sensitive information, only where strictly necessary and permitted by applicable law.

Such processing may occur, for example, in the context of:

- recruitment or employment obligations (e.g., health and safety requirements, workplace accommodations, mandatory checks);
- compliance with legal or regulatory obligations (including AML/CFT, background or integrity checks where required by law);
- the establishment, exercise or defence of legal claims; or
- where you have provided your explicit consent, where required.

This data is subject to enhanced technical and organisational safeguards and is accessible only to authorised personnel on a strict need-to-know basis.

With respect to employee data, specific legal bases apply as described in the section “HR and recruitment” below

6 Who we share information with

In the course of providing our services and conducting our business operations, InvesTRe S.A. may disclose or transfer your personal data to trusted third parties (the “**Recipients**”) where this is necessary to deliver our services, comply with legal or regulatory obligations, protect our legitimate interests, or where you have provided your consent. Certain Recipients may rely on authorised subcontractors, affiliates or agents (“**Sub-Recipients**”) to support the delivery of their services, subject to equivalent data protection and confidentiality obligations.

These Recipients/Sub-Recipients may include:

Service Providers

We engage reputable Service Providers to support the effective delivery of our services and business activities. These may include, without limitation, IT and cloud providers, hosting companies, website analytics providers, payment processors, email distribution services, event vendors, procurement providers, recruitment firms, financial intermediaries and professional advisers.

Where certain website or operational functionalities require it, limited personal data may be shared strictly on a need-to-know basis.

Depending on the context and the nature of the processing, Service Providers may act either as data processors on our behalf or as independent data controllers where they process personal data for their own legal, regulatory or professional purposes. Where acting as processors, they are contractually bound to:

- process personal data solely on our documented instructions;
- use such data only to provide services to us;
- implement appropriate technical and organisational security measures; and
- comply with strict confidentiality and data protection obligations.

Legal, Regulatory and Public Authorities

We may disclose personal data where required to comply with applicable laws, regulations, regulatory requests, subpoenas, court orders or lawful instructions from public authorities, or where necessary to:

- establish, exercise or defend legal claims;
- fulfil tax, accounting or reporting obligations;
- prevent or investigate fraud or unlawful activities; or
- protect the rights, property or safety of InvesTRe S.A., our clients, employees or others.

Recipients may include governmental, judicial, prosecution or regulatory authorities, official national registers, tax authorities, law enforcement agencies, banking institutions, notaries, domiciliation agents, auditors and professional advisers.

In certain cases, both InvesTRe S.A. and the recipient may act as independent data controllers.

Event Partners

Where you register for or attend events organised or co-organised by us, your personal data may be shared with partners or vendors involved in the organisation and management of such events, subject to appropriate safeguards.

Business Transfers

In the event of a merger, acquisition, restructuring, financing, or sale of all or part of our business or assets, personal data may be transferred to relevant parties involved in the transaction, subject to confidentiality and legal safeguards.

Consent-Based Sharing

Where required, we may share your personal data with selected marketing, advertising or social media partners, or for other new purposes, based solely on your explicit consent. You may withdraw your consent at any time through our preference settings or cookie banner.

Aggregated and Anonymised Data

We may use, publish, share or commercialise aggregated or anonymised information that cannot reasonably be linked to any individual for research, statistical or reporting purposes.

Sub-processors list

Our sub-processors list is accessible [here](#).

7 Cookie Notice

For the avoidance of doubt, this Privacy Notice must be read together with our Cookies Notice, which forms an integral part of our data protection framework – available [here](#).

Where you accept this Privacy Notice in the context of using our Website or digital services and/or application, such acceptance also covers the applicable Cookies Notice, subject to your specific consent choices made via our cookie banner or preference settings.

8 Automated Decision Making

Certain processing activities, including Anti-Money Laundering (AML) and Know Your Customer (KYC) controls, may involve the use of automated tools designed to support risk assessment and compliance checks.

Decisions are not based solely on automated processing without appropriate safeguards. Where automated processing contributes to a decision that produces legal or similarly significant effects — for example a refusal to onboard or provide services — such decision is subject to internal review mechanisms, including human oversight where appropriate.

Data subjects have the right, in accordance with applicable data protection law, to request human intervention, to express their point of view and to contest a decision where they consider that automated processing has materially affected the outcome. Certain information relating to AML/CFT assessments may however be restricted where disclosure would undermine regulatory obligations or the prevention of financial crime.

To exercise these rights, please contact privacy@investre.eu.

9 Data processing outside the EU

Recipients of your personal data may be located inside or outside the European Economic Area (EEA), including where we use service providers, partners or affiliates established abroad.

Where personal data is transferred to a country that is not recognised by the European Commission as providing an adequate level of protection, we implement appropriate safeguards in accordance with Chapter V of the GDPR, which may include standard contractual clauses or other legally recognised transfer mechanisms.

You may request further information regarding these safeguards by contacting us at privacy@investre.eu

10 Security of Personal Data

In connection with the provision of our services and business activities, we implement data protection by design and by default and apply industry-standard organisational, technical and physical security measures to ensure the confidentiality, integrity and availability of personal data and to protect it against unauthorised or accidental access, loss, alteration, disclosure or destruction.

These measures include, as appropriate:

- **Access controls:** strict logical and physical access restrictions based on the principle of least privilege and role-based authorisation;
- **Secure infrastructure:** protected IT systems, networks and hosting environments, including encryption, pseudonymisation where relevant, endpoint protection and secure configuration standards;
- **Monitoring and testing:** logging, continuous monitoring, vulnerability management, and regular security assessments and audits to identify and remediate risks;
- **Data minimisation and retention controls:** collection and retention limited to what is necessary for the defined purposes, with secure deletion or anonymisation where data is no longer required;
- **Employee awareness and training:** mandatory confidentiality obligations and regular training on data protection, information security and secure handling practices;
- **Incident response and business continuity:** documented procedures to detect, contain, investigate and remediate security incidents or personal data breaches, including notification processes where required by law;
- **Operational safeguards:** secure handling of hard-copy documents and restrictions on the remote use of physical files.

While we apply appropriate technical and organisational security measures consistent with industry standards and applicable legal requirements, no system of transmission or storage can be guaranteed to be completely secure.

Accordingly, although we strive to protect personal data at all times and continuously review and enhance our security controls, we cannot eliminate all risks associated with data processing.

11 Your Data Protection Rights

As an individual whose personal information is processed by InvesTRe S.A., you have certain rights regarding the protection and control of your data. We are committed to upholding these rights and ensuring that you can exercise them effectively:

- **Right to Access:** Data subjects can request access to their personal data and obtain information about how the data is being processed.
- **Right to Rectification:** Data subjects can request correction of inaccurate or incomplete personal data.
- **Right to Erasure** ("Right to be Forgotten"): Data subjects can request the deletion of personal data when it is no longer necessary for the purposes for which it was collected or if they withdraw consent.
- **Right to Restrict Processing:** Data subjects can request the restriction of processing in certain circumstances.
- **Right to Data Portability:** Data subjects can request to receive their personal data in a structured, commonly used, and machine-readable format and have the right to transmit that data to another controller.
- **Right to Object:** Data subjects can object to processing based on legitimate interests, direct marketing, and processing for purposes of scientific or historical research and statistics.
- **Right not to be subject to Automated Decision-Making:** Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.
- **Right to lodge a complaint with the supervisory authority** - <https://cnpd.public.lu/en.html>.

The Luxembourg supervisory authority is:

Commission Nationale pour la Protection des Données (the "CNPD")

Address: 15, Boulevard du Jazz, L-4370 Belvaux, Luxembourg

Tel: (+352) 26 10 60 -1

Website: <https://cnpd.public.lu/>

Please also note that:

- You can revoke consent to our marketing communications at any time using the unsubscribe link contained in each email.
- You can give or revoke consent to our referral programs/our events any time by emailing: privacy@investre.eu

To exercise these rights named above you may contact us at any time via email to privacy@investre.eu

12 Retention period and Deleting personal data

We retain personal data only for as long as necessary for the purposes for which it was collected and processed.

In particular, personal data may be retained:

- for the duration of any pre-contractual or contractual relationship with you or the organisation you represent, including for legitimate business and operational purposes;
- for as long as required or permitted by applicable laws and regulations (including data protection, accounting, tax, regulatory or statutory limitation requirements); and
- where necessary for the establishment, exercise or defence of legal claims.

Where no specific retention period applies, personal data is kept only until the relevant purpose or legal basis for processing no longer exists.

Upon closure of your account, termination of the relationship, withdrawal of consent (where processing is based on consent), or expiry of the applicable retention period, we take appropriate steps to securely delete or anonymise personal data so that it can no longer be associated with you.

Anonymised data that can no longer be linked to an identifiable individual may be retained without time limitation.

You can request for your data to be deleted (in accordance with applicable law) by using this [Data Deletion online form](#)

13 Blockchain and tokenisation

Where tokenisation services result in the recording of personal data on distributed ledger technology (DLT), InvesTRe S.A. ensures that personal data is stored 'off-chain' to the extent possible.

Only pseudonymised identifiers are recorded on-chain. In particular, on-chain records contain hashed or technical identifiers (including wallet identifiers) that do not directly identify a data subject. The correspondence between such identifiers and the relevant client or investor is maintained off-chain in InvesTRe S.A.'s internal systems, subject to appropriate technical and organisational safeguards.

This approach supports compliance with GDPR principles, including data minimisation and privacy by design, and facilitates the effective exercise of data subject rights.

Where a data subject exercises their right to rectification, any inaccurate personal data can be corrected off-chain without altering the integrity or immutability of the blockchain records.

Where a data subject exercises their right to erasure, InvesTRe S.A. may delete or irreversibly sever the off-chain mapping between the on-chain identifier and the data subject, subject to applicable legal and regulatory retention obligations (including accounting and AML record-keeping requirements). In such cases, the remaining on-chain data no longer relates to an identifiable natural person.

14 HR and recruitment

When you apply for a position through our website or otherwise provide your application, we collect and process personal data necessary to assess your candidacy. This may include your contact details, professional experience, education, qualifications, skills, and any information contained in your CV, cover letter or supporting documents.

We use this data solely to:

evaluate your application and suitability for employment;

- communicate with you throughout the recruitment process;
- prepare related documentation (e.g., interview correspondence or offers); and
- where permitted by law, carry out background or compliance checks.

Employees and HR Management

For employees and staff members, we process personal data as necessary for the management of the employment relationship, including:

- recruitment and onboarding;
- personnel administration, payroll, benefits and training;
- performance management and career development;

- compliance, risk management and internal governance;
- workplace security and IT systems management; and
- the establishment, exercise or defence of legal rights.

Further details are available in our internal employee privacy documentation provided to staff.

Retention

HR and recruitment data is retained only for as long as necessary for the relevant employment or recruitment purposes and in accordance with applicable legal and statutory retention requirements. Data is securely deleted or anonymised once no longer required.

15 Changes to this Privacy Notice

We may update this **Privacy Notice** from time to time to reflect changes in applicable laws, regulatory requirements, our processing activities, or our data protection practices.

Where changes are material and significantly affect your rights or the way we process your personal data, we will take appropriate steps to inform you, for example by email, through our website or via our application, as appropriate.

The updated version will be published on our website/applications and will indicate the date of the latest revision. We encourage you to review this **Privacy Notice** periodically to stay informed about how we protect your personal data.

16 Contact us

If you have any questions or concerns about our use of your information or regarding our **Privacy Notice**, you may contact us by the following contact details:

InvesTRe S.A.
Attn: Data Protection Officer
209 Rue des Romains, Bertrange, L-8041, Luxembourg
Email: to privacy@investre.eu

Version History

Version	Summary of
1.0	Replaces previous Version 1.1.2 of the Privacy Policy Moniflo Web (30/09/2025) and Version 3.1.1 (29/09/2025)

--	--