INOVEXUS

Privacy Policy

Data Protection Declaration for Inovexus Investment Platform

EFFECTIVE DATE

September 8th, 2026

LAST UPDATED

August 31st, 2026

VERSION

7.1

Quick Reference Card

Your Key Rights & How to Exercise Them

- **Access Your Data**: Email dpo@inovexus.com with "Data Access Request." | *Response within 15 days*
- **Delete Your Data**: Email dpo@inovexus.com with "Deletion Request." | *Response within 15 days*
- **Correct Your Data**: Update your profile settings or email dpo@inovexus.com. | *Response within 15 days*
- **Export Your Data**: Email dpo@inovexus.com with "Data Export Request." | *Response within 15 days*
- **Stop Marketing**: Click "unsubscribe" in any marketing email or update your email preferences. | *Immediate*
- **Contest an AI Decision**: Email dpo@inovexus.com with "Human Review Request." | *Response within 15 days*

Cookie Categories & Your Choices

- **Strictly Necessary Cookies**: These cookies are required for the Platform to operate and cannot be disabled through the Platform. They may be used for authentication and login sessions, account security, fraud and abuse prevention, session management, maintaining your preferences and settings, load balancing, and other functions necessary to provide and secure the Platform.

- **Analytics Cookies**: These cookies help us understand how users interact with the Platform and improve its performance and functionality. They may collect information such as pages or features viewed, clicks and interactions, session duration, navigation patterns, device and browser information, approximate location, referral sources, and information about errors or performance issues. We use this information to measure usage, identify trends, diagnose technical issues, improve the Platform, and understand which features are most useful. You can request that we disable or limit analytics cookies by emailing dpo@inovexus.com.

- **Marketing Cookies**: These cookies may be used to understand and measure the effectiveness of our marketing activities, deliver or personalize marketing communications and advertising, measure conversions and campaign performance, and understand how users interact with our marketing content. They may collect information such as pages visited, interactions with advertisements or marketing communications, referral sources, campaign identifiers, and conversion or engagement information. Where applicable, these cookies may allow us or our advertising partners to recognize your browser or device across websites or services for advertising and measurement purposes. You can request that we disable or limit marketing cookies by emailing dpo@inovexus.com.

Emergency & Privacy Contacts

- **Data Breach / Security Issue:** Email dpo@inovexus.com
- **Privacy Complaint / Data Protection Request:** Email dpo@inovexus.com
- **Regulatory Authority:** Commission Nationale de l'Informatique et des Libertés (CNIL), France - www.cnil.fr

Table of Contents

01	Data Controller and Contact Information	pg.04
02	Scope and Application	pg.06
03	Definitions	pg.08
04	Categories of Personal Data	pg.09
05	Purposes and Legal Basis for Processing	pg.11
06	User Journey: Your Data Through Our Platform	pg.15
07	Automated Decision-Making and Profiling	pg.19
08	Data Recipients and Transfers	pg.22
09	International Data Transfers (Focus: US Transfers)	pg.26
10	Data Retention and Deletion	pg.30
11	Technical and Organizational Security Measures	pg.34
12	Your Rights as a Data Subject	pg.38
13	Complete Cookie Policy	pg.43
14	Special Categories of Personal Data	pg.49
15	Data Protection for Minors	pg.51
16	Changes to This Privacy Policy	pg.53
17	Complaint Rights	pg.55
18	Final Provisions	pg.57
19	Version Control and Archive	pg.60

Appendices

INOVEXUS

01

Data Controller and Contact Information

1.1 Data Controller

Inovexus Société par Actions Simplifiée (SAS)
Legal Form: Société par Actions Simplifiée
Registration Number (SIREN/SIRET): 843 313 735,
RCS Registration: RCS Paris B 843 313 735
VAT ID: FR 21 843313735
Registered Address: 4 Rue Royale, 75008 Paris, France
Email: dpo@inovexus.com
Website: https://www.inovexus.com

Inovexus determines the purposes and means of the processing of your personal data and is therefore the "controller" within the meaning of the GDPR.

1.2 Data Protection Officer

Independent Contact Email: dpo@inovexus.com
Postal Address: 4 rue Royale, 75008 Paris, France

Our DPO is available for all questions relating to this privacy policy and the exercise of your data protection rights.

INOVEXUS

02

Scope and Application

2.1 Territorial Scope

This privacy policy applies to the processing of personal data in the context of the activities of Inovexus, regardless of whether the processing takes place in the European Union or not, insofar as the processing relates to:

- The offering of goods or services to data subjects in the European Union; and/or
- The monitoring of behavior of data subjects within the European Union.

2.2 Material Scope

This policy covers all personal data processing carried out by or on behalf of Inovexus, including:

- Inovexus investment platform (platform.inovexus.com/community.inovexus.com)
- Main corporate website (www.inovexus.com)
- Mobile applications (iOS and Android)
- Email marketing and WhatsApp/phone communications
- Event management and execution
- Community management and networking
- Investment sourcing, processing, and administration
- Due diligence, AML/KYC and compliance activities
- Customer support and service delivery
- Research and development activities
- Marketing, analytics, and business development

2.3 Excluded Areas

This policy does not apply to:

- Processing of employee data (covered by a separate employee privacy notice)
- Processing by independent third parties with their own privacy policies (though our sharing is described in Section 8)
- Processing of purely public information not combined with other personal data

2.4 Children's Privacy

Key Takeaway: Our investment services are not intended for anyone under 18. We delete accounts if we discover underage use.
Age Restriction: Inovexus platform and services are intended for adults aged 18 and over. Investment services, financial products, and community features are not suitable for minors.
No Intentional Collection: We do not knowingly collect personal data from children under 18. Our registration process includes age verification, and terms of service require users to confirm they are 18+.

Discovery and Deletion Process:

If we learn a user is under 18:
- Immediately suspend account access
- Contact parent/guardian if possible
- Delete all personal data within 30 days
- No retention except for security/fraud prevention (anonymized)

Verification Methods:
- Self-declaration during registration
- ID verification during KYC process
- Automated flagging of suspicious age-related indicators

If you believe a child has provided personal data to us, please contact dpo@inovexus.com immediately with "Minor Account" in the subject line.

03

Definitions

“Personal Data”, “Processing”, “Data Subject”, “Controller”, “Processor”, “Profiling” and other key terms have the meanings given in Articles 4 and 9 GDPR.

INOVEXUS

04

Categories of Personal Data

We process the following categories of personal data, where applicable and depending on your interactions with the Platform:

- **Identity and Contact Data**: Name, date and place of birth, nationality, gender where provided, postal address, email address, telephone number, profile photograph, and other contact details.
- **Professional and Career Data**: Employment history, job title, role, company or organization, industry, professional experience, education, skills, professional interests, LinkedIn and similar professional profile information, and information contained in professional biographies or profiles.
- **Financial and Investment Data**: Bank account and payment details where required, investment history, investment preferences, investment capacity, source of funds or wealth where required, risk profile, transaction information, tax identifiers, and AML/KYC documentation.
- **Platform and Technical Data**: Account credentials, account identifiers, IP address, browser and device information, device identifiers, operating system, authentication information, cookies and similar technologies, login activity, usage logs, pages and features accessed, interactions, and technical or diagnostic information.
- **Communication and Marketing Data**: Communications with us, email history, marketing preferences, event registrations and participation, survey and feedback responses, community posts and interactions, support requests, and other information you provide when communicating with us.
- **Transaction and Subscription Data**: Membership or subscription type, billing status, subscription dates, payment status, transaction records, invoices, and information relating to purchases or membership services. Payment card details may be processed directly by our payment service providers rather than stored by us.
- **Event and Community Data**: Information relating to your participation in events, workshops, community activities, registrations, attendance, networking interactions, and content or information you voluntarily share with other community members.
- **Marketing and Attribution Data**: Information used to measure and understand the effectiveness of our marketing activities, such as campaign identifiers, referral sources, advertising interactions, website visits, conversions, and engagement with marketing communications.
- **User-Generated Content**: Information you voluntarily submit or publish through the Platform, including comments, posts, profiles, messages, feedback, applications, documents, and other content.
- **Compliance and Verification Data**: Information necessary to comply with legal and regulatory obligations, including identity verification, AML/KYC checks, sanctions screening, fraud-prevention checks, PEP screening, and information required to establish or verify your eligibility to use particular services.
- **Special Categories of Personal Data (limited; see Section 14)**: Where legally permitted and necessary, we may process limited special-category or sensitive information, such as information relating to health or accessibility requirements for events, or other sensitive information where required by law or provided voluntarily for a specific purpose. We do not intentionally collect sensitive personal data unless there is a lawful basis and a specific need to do so.

INOVEXUS

05

Purposes and Legal Basis for Processing

We process your personal data only where a valid legal basis under Article 6 and, where relevant, Article 9 GDPR applies.

5.1 Contract Performance (Art. 6(1)(b) GDPR)

- **Platform Account Management**: To create, maintain, authenticate, operate, and secure your account; manage your profile and preferences; and provide access to the Platform and its features.
- **Investment Services**: To facilitate your participation in investment opportunities, assess and process applications, connect investors with relevant opportunities, facilitate investment-related processes, manage investor relationships, and provide post-investment information and reporting.
- **Membership and Subscription Management**: To provide and manage your membership or subscription, determine your access level, process membership-related transactions, manage billing and subscription status, and provide the services included with your membership.
- **Community Services**: To provide access to community features, networking opportunities, mentoring, events, educational resources, and other services available through the Platform.
- **Customer Support:** To respond to enquiries, provide customer and technical support, troubleshoot issues, and assist you in using the Platform and its services.
- **Service Communications**: To send communications necessary to provide and administer the services you have requested, including account notifications, service updates, investment-related communications, event information, and other operational messages.
- **Personalization of Services**: To use information associated with your account to provide services, opportunities, content, or community experiences that are relevant to your profile, preferences, and use of the Platform, where this processing is necessary to provide the services you have requested.

5.2 Legal Obligations (Art. 6(1)(c) GDPR) and Investment Regulation

We process personal data where necessary to comply with applicable EU, French, and other national financial, investment, anti-money laundering, tax, and regulatory requirements, including, where applicable (non-exhaustive):

- **MiFID II investor protection requirements**, including suitability and appropriateness assessments and related record-keeping obligations
- **EU and national AML/CTF requirements**, including KYC, verification of identity and beneficial ownership, source of funds or wealth checks, PEP and sanctions screening, and suspicious activity reporting where required
- **Tax reporting obligations**, including CRS, FATCA, and applicable local tax laws
- **Record-keeping obligations** under applicable commercial, tax, financial-market, and regulatory laws

Examples of processing carried out for these purposes include:

- Collecting and verifying identity, beneficial ownership, financial situation, and investment experience
- Conducting KYC, AML, sanctions, and PEP checks
- Retaining transaction data, contracts, communications, and compliance records for the periods required by applicable law, which may in certain circumstances be **5–10 years or longer**
- Sharing relevant personal data with competent authorities, such as the **AMF, TRACFIN, tax authorities, courts, or other regulators**, where required or permitted by law

Where applicable, statutory or regulatory retention requirements may require us to retain personal data for a specified period even if you request its deletion. During such periods, these obligations may limit or delay certain rights, including your rights to **erasure, objection, restriction of processing, or data portability**, to the extent permitted by applicable law.

5.3 Legitimate Interests (Art. 6(1)(f) GDPR)

Where we rely on legitimate interests, we conduct and periodically review a balancing test to assess whether our legitimate interests are proportionate and do not override your rights and freedoms.

Examples include:

1. **Platform Security and Fraud Prevention**
   - **Interest**: Protecting the security, integrity, and availability of the Platform and its users; detecting, preventing, and investigating fraud, abuse, unauthorized access, and other security threats.
   - **Necessity**: Security monitoring and fraud-prevention measures are necessary to operate a secure Platform and protect users and our services.
   - **Balancing**: We use proportionate technical and behavioral information, apply appropriate safeguards, limit access, and retain information only for as long as reasonably necessary.
   - **Conclusion**: Where the processing is necessary and proportionate, our legitimate interest in protecting the Platform and its users is not overridden by your rights. You may not be able to opt out of processing that is strictly necessary for security or fraud prevention.

2. **Business Analytics and Service Improvement**
   - **Interest**: Understanding how the Platform is used, identifying technical or usability issues, improving features, performance, reliability, and the overall user experience.
   - **Necessity**: Certain analytics are necessary to understand Platform performance and improve our services. Where appropriate, we use aggregated or pseudonymized information and avoid using more personal data than necessary.
   - **Balancing**: We apply appropriate safeguards, limit access and retention, and provide an opt-out where required or technically feasible. Where consent is legally required for particular analytics or tracking technologies, we will obtain consent instead.
   - **Conclusion**: Where legitimate interests are an appropriate legal basis, the processing is proportionate and safeguards are applied to protect your rights and freedoms.

3. **Relevant Opportunity Recommendations**
   - **Interest**: Curating and presenting investment opportunities, mentoring opportunities, events, and other Platform opportunities that may be relevant to your professional interests, stated preferences, investment interests, or participation in the community.
   - **Necessity**: Using information you provide to the Platform can help us provide more relevant opportunities and services and improve the usefulness of the Platform.
   - **Balancing**: We consider the professional context, the information reasonably expected to be used for this purpose, the nature and sensitivity of the data involved, and the safeguards and preferences available to users. We do not use sensitive personal data for this purpose unless permitted by law and an appropriate legal basis applies.
   - **Conclusion**: Where our legitimate interest is the appropriate legal basis, we will process information in a proportionate manner and provide an opportunity to object where required.

You may object to processing based on our legitimate interests at any time, as described in **Section 12**. Where you object, we will stop the relevant processing unless we can demonstrate **compelling legitimate grounds** that override your interests, rights, and freedoms, or the processing is necessary for the establishment, exercise, or defence of legal claims.

5.4 Consent (Art. 6(1)(a) GDPR)

We rely on your consent where required by applicable law and where you have a genuine choice, including for:

- **Non-essential cookies and similar technologies**, including certain analytics, advertising, and tracking technologies where consent is required.
- **Certain marketing communications**, particularly where consent is required for communications to individuals who are not existing customers or where another lawful basis for marketing is not available.
- **Advanced analytics and profiling** that are not strictly necessary to provide, operate, or secure the Platform.
- **Optional networking and data sharing**, where you choose to make certain profile or other information available to other community members.
- **Event photography, video recording, and media use**, where you are identifiable and consent is the appropriate legal basis.

Where we rely on consent, it will be obtained through a clear affirmative action and will be specific, informed, and freely given. You may withdraw your consent at any time. Withdrawal will not affect the lawfulness of processing carried out before withdrawal.

See **Section 5.1.5 (Consent Management) and Section 13 (Cookies and Similar Technologies)** for further details.

06

User Journey: Your Data Through Our Platform

Key Takeaway: This section explains how your personal data may be collected, used, shared, and retained at different stages of your interaction with our Platform.

Stage 1: Account Creation

Data Collected: Name, email address, password or authentication credentials, and basic contact information.

Why: To create and secure your account, provide access to the Platform, authenticate you, and communicate with you about your account.

Stored Where: Personal data is stored using our hosting and infrastructure providers in accordance with our security and data-protection requirements. Where applicable, we use appropriate technical and organizational safeguards, including access controls and encryption.

Legal Basis: Contract performance (Art. 6(1)(b) GDPR) and, where applicable, legitimate interests (Art. 6(1)(f) GDPR).

Retention: Account information is retained for the duration of your account and thereafter for as long as necessary to comply with applicable legal, regulatory, security, dispute-resolution, and legitimate business requirements.

Stage 2: Profile Building

Data Collected: Professional background, employment information, investment preferences, investment experience, areas of interest, and information from professional-profile integrations such as LinkedIn, where you choose to connect them.

Why: To provide relevant Platform services, personalize your experience, facilitate community networking, and identify potentially relevant investment opportunities, events, mentors, or other community resources.

AI Analysis Explained: Where AI-powered matching or recommendation features are used, our systems may analyze information you provide, such as preferred sectors, geographic interests, investment preferences, investment experience, and other relevant profile information, to identify potentially relevant opportunities or connections.

These systems are intended primarily to match information you have provided with characteristics of opportunities or other Platform participants. We do not use AI-based matching to make decisions that produce legal or similarly significant effects about you unless we have a lawful basis to do so and provide any rights and safeguards required by applicable law.

Legal Basis: Contract performance (Art. 6(1)(b) GDPR), legitimate interests (Art. 6(1)(f) GDPR), and, where applicable, consent (Art. 6(1)(a) GDPR).

Retention: Profile information is retained while your account remains active and thereafter for as long as necessary for applicable legal, regulatory, security, dispute-resolution, and legitimate business purposes.

Stage 3: KYC and Verification

Data Collected: Government-issued identification, proof of address, beneficial ownership information, financial information, source of funds or wealth documentation, and results of applicable KYC, AML, sanctions, and PEP screening.

Why: To comply with applicable legal and regulatory obligations, verify identity and eligibility, prevent fraud and financial crime, and meet applicable AML/CTF and investment-related requirements.

Third Parties: Where required, we may use specialized identity-verification, KYC, AML, sanctions-screening, or compliance service providers. The specific providers used may change over time. Where applicable, information about relevant processors is provided in our list of third-party service providers or upon request.

Storage: Verification information is stored and processed using appropriate technical and organizational security measures and access controls. Access is limited to personnel and service providers who require the information for legitimate business, legal, or regulatory purposes.

Legal Basis: Legal obligation (Art. 6(1)(c) GDPR) and, where applicable, legitimate interests (Art. 6(1)(f) GDPR).

Retention: KYC and compliance information is retained for the periods required by applicable AML/CTF, financial-services, tax, and other regulatory requirements. Depending on the applicable requirement, certain records may need to be retained for **5–10 years or longer**.

Stage 4: Investment Processing

Data Shared With: Depending on the investment structure and services involved, relevant information may be shared with:

- Portfolio companies, investment vehicles, administrators, or other entities involved in maintaining investor or shareholder records
- Service providers involved in processing investments, payments, subscriptions, or distributions
- Professional advisers and other service providers where necessary to provide the relevant services
- Co-investors or community members where you have chosen to make relevant professional or profile information available for networking purposes
- Tax authorities, regulators, courts, or other competent authorities where required or permitted by law.

Purpose: To facilitate investment transactions and related administrative processes, maintain appropriate legal and ownership records, manage investor relationships, process payments or distributions, provide reporting, and comply with legal and regulatory obligations.

Safeguards: We seek to limit disclosures to information reasonably necessary for the relevant purpose and apply appropriate contractual, technical, and organizational safeguards to protect personal data.

Legal Basis: Contract performance (Art. 6(1)(b) GDPR), legal obligation (Art. 6(1)(c) GDPR), and, where applicable, legitimate interests (Art. 6(1)(f) GDPR).

Stage 5: Ongoing Relationship

Communications: Depending on your relationship with us and your preferences, we may send service and account communications, investment and portfolio updates, community communications, newsletters, educational content, and event invitations.

Analytics: We may analyze Platform usage, feature engagement, communication engagement, and other service-performance information to operate, secure, maintain, and improve the Platform. Where consent is legally required for particular analytics or tracking technologies, we will obtain consent.

Legal Basis: Contract performance for necessary service communications; consent where required for marketing or non-essential tracking; and legitimate interests where appropriate for operational analytics, service improvement, security, and related purposes.

Control: You may manage your marketing and communication preferences and withdraw consent where processing is based on consent. You may also object to processing based on legitimate interests where applicable.

Retention: Personal data is retained for as long as necessary for the relevant purpose and thereafter in accordance with applicable legal, regulatory, security, dispute-resolution, and legitimate business requirements.

Stage 6: Startup Confidential Information Protection

Key Takeaway: We take measures to protect confidential information relating to startups, investment opportunities, and other business information shared through the Platform.

Data Protected: Depending on the services provided, this may include pitch decks, financial projections, business plans, due-diligence materials, cap tables, commercial information, strategic plans, intellectual property information, and other confidential business information provided by startups or their representatives.

Access Controls:
- Access is limited to authorized personnel, advisers, investors, community members, or service providers who require access for a legitimate purpose
- Permissions may be restricted based on the relevant startup, investment opportunity, role, or service
- We use access controls and other appropriate measures designed to prevent unauthorized access, disclosure, alteration, or loss
- Where technically available, access and activity may be logged for security, compliance, and audit purposes
- Access may be removed or adjusted when it is no longer required.

Technical and Organizational Safeguards:
We maintain appropriate technical and organizational measures designed to protect confidential information, which may include encryption, authentication controls, access restrictions, secure storage, monitoring, backups, security testing, and employee security procedures. The specific safeguards may vary depending on the system, service provider, and nature of the information.

Legal and Contractual Protections:
- Personnel and relevant contractors may be subject to confidentiality obligations
- Third-party service providers may be subject to contractual confidentiality and data-protection obligations
- Investors, community members, and other users may be required to agree to applicable confidentiality or terms-of-use obligations before accessing certain startup information
- We may investigate and take appropriate action in response to unauthorized access, use, or disclosure.

Retention: Confidential startup information is retained for as long as reasonably necessary for the relevant investment, business, contractual, legal, or regulatory purpose. Information may be retained after an investment or relationship ends where necessary to comply with legal or regulatory obligations, resolve disputes, maintain appropriate records, or protect legitimate business interests.

INOVEXUS

07

Automated Decision-Making and Profiling

7.1 MatchAI and ScoutAI Systems

We use AI-assisted systems, including **MatchAI** and **ScoutAI**, to help analyze information and provide recommendations relating to investment opportunities and Platform services.

Depending on the service and information available, these systems may assist with:

- **Investor–Startup Matching (MatchAI)**
- **Startup Screening and Assessment (ScoutAI)**
- **Investment Opportunity Prioritization**
- Recommending relevant opportunities, community members, events, or other Platform resources.

These systems may consider information such as your stated investment preferences, professional background, investment experience, areas of interest, and characteristics of available opportunities.

The systems may rank or prioritize opportunities based on their predicted relevance to you. This can affect the order in which opportunities are presented to you, but it does not prevent you from accessing or considering other available opportunities where those opportunities are otherwise available to you.

AI-assisted recommendations do not replace human judgment in investment decisions. You remain responsible for deciding whether to pursue or make an investment. Where an investment decision requires human assessment or approval, that decision is not made solely by the AI system.

7.2 Automated Decision-Making and Your Rights

Our AI-assisted matching and recommendation systems are intended primarily to provide recommendations and organize information. They are not intended to make decisions based solely on automated processing that produce legal effects or similarly significant effects concerning you.

Where applicable law provides you with rights in relation to automated decision-making or profiling, including the right to obtain meaningful information about the logic involved, express your point of view, contest a decision, or request human intervention, we will provide those rights in accordance with applicable law.

If you believe an AI-assisted recommendation or profile assessment is inaccurate, unfair, or based on incorrect information, you may contact dpo@inovexus.com with "**Human Review Request**" in the subject line. Please identify the recommendation or issue you would like reviewed and, where possible, explain why you believe it is inaccurate or inappropriate.

We will review requests in accordance with applicable law and our internal review procedures.

7.3 AI Transparency and Safeguards

We take reasonable measures to ensure that AI-assisted systems are operated responsibly and that personal data used by these systems is processed in accordance with applicable data-protection requirements.

Depending on the system and its use, safeguards may include:

- **Human oversight**: Appropriate human oversight of AI-assisted processes, particularly where outputs may materially influence investment-related activities.
- **Data minimization**: Using information relevant to the particular matching, recommendation, or assessment purpose.
- **Accuracy**: Taking reasonable steps to maintain accurate profile information and providing mechanisms for users to correct inaccurate personal data.
- **Access controls**: Restricting access to AI systems and their underlying data to authorized personnel and service providers.
- **Monitoring**: Monitoring system performance and outputs for significant errors, inappropriate results, or other issues.
- **Model governance**: Maintaining appropriate documentation and version controls for material changes to AI-assisted systems where applicable.
- **Testing and review**: Conducting appropriate testing and review of AI-assisted systems, including consideration of potential bias and discriminatory outcomes where relevant.
- **Human intervention**: Providing appropriate human oversight and review mechanisms where required by applicable law.

AI systems may be updated, improved, retrained, or replaced from time to time. The specific models, techniques, data sources, and safeguards used may therefore change over time.

For questions about AI-assisted processing, to request correction of information used by our systems, or to request human review where applicable, contact dpo@inovexus.com.

INOVEXUS

08

Data Recipients and Transfers

8.1 Internal Recipients

Access to personal data within Inovexus is limited to persons who need it to fulfil their tasks, e.g.:

- Investment committee and deal teams
- Compliance and legal
- Customer support and operations
- Technology/security teams
- Marketing and growth (for permitted uses only).

Role-based access controls apply.

8.2 External Processors

We use selected third-party service providers (our data processors) to provide, maintain, secure, and improve the Platform and related services. These providers process personal data only as necessary to provide their contracted services and subject to appropriate contractual and security requirements.

The categories of processors we may use include:

Processor / Service	Data Processed	Purpose
Disco	Name, email address, profile information, community content and interactions	Community platform and networking services
Affinity	Contact information, professional information, investment-related information, and interaction records	CRM, relationship management, and investor-related analytics
Mailchimp (Intuit)	Name, email address, communication preferences, and email engagement information	Marketing emails, newsletters, and communications
Google Workspace	Emails, documents, calendar information, and other information stored or communicated through our workspace	Business collaboration, communication, and productivity
Zoom	Name, email address, meeting information, and recordings where enabled	Video conferencing, meetings, and events
Stripe	Payment and transaction information	Payment processing and subscription management

Processor / Service	Data Processed	Purpose
Zapier	Contact information, form information, and workflow-related data	Automation and integration between services
DocuSign	Contract information, documents, signatures, and related identification information	Electronic signatures and document management
Calendly	Name, email address, scheduling information, and calendar-related information	Meeting scheduling
Intercom	Name, email address, support communications, and information provided during support interactions	Customer support and communication
Datadog	Technical information, system logs, performance information, and diagnostic data	Platform monitoring, security, and performance management
KYC / Verification Providers	Identity documents, verification information, and compliance-screening results where applicable	Identity verification, KYC, AML/CTF, sanctions, and PEP screening
Roundtable	Information necessary to provide the relevant Roundtable service, where applicable	Community, event, networking, or related services
Elevatorfy	Founder profile information, professional information, contact details, and information provided by founders for networking or collaboration	Founder networking, connections, collaboration, and related founder-to-founder services
Supabase	Account information, profile information, authentication data, application data, Platform activity, and other personal data stored or processed through our databases and application infrastructure.	Database hosting, authentication, application infrastructure, and secure storage

The specific providers we use may change from time to time as our Platform and services develop. Where required by applicable law, we will enter into appropriate data-processing agreements with processors and ensure that suitable safeguards are in place for international transfers of personal data.

Where personal data is transferred outside the European Economic Area (EEA), we will use an appropriate transfer mechanism where required, such as an adequacy decision, Standard Contractual Clauses (SCCs), or another lawful transfer mechanism.

We assess the security and data-protection practices of relevant service providers on a risk-based basis and require appropriate technical and organizational measures to protect personal data.

Information about specific processors, their processing activities, and applicable international transfer safeguards may be provided where required by applicable law or upon reasonable request.

Note: Complete processor register including all sub-processors available upon request at dpo@inovexus.com.

8.2.1 Sub-Processors and Processing Chains

Our primary processors may engage their own sub-processors, including cloud infrastructure, hosting, security, analytics, communications, and other technology providers, as necessary to provide their services.

We:

- Maintain appropriate records of relevant processors and sub-processors based on our vendor-management processes
- Require appropriate data-protection and confidentiality obligations to apply to relevant sub-processors
- Assess relevant sub-processors and processing arrangements on a risk-based basis
- Require appropriate safeguards for international transfers of personal data, including Standard Contractual Clauses (SCCs) or other lawful transfer mechanisms where required.

Where required by applicable law, we will provide information about relevant processors and material changes to sub-processing arrangements and, where applicable, provide an opportunity to object.

You may request information about our current processors and relevant sub-processors by contacting dpo@inovexus.com.

8.3 Third-Party Controllers

In certain circumstances, personal data may be shared with **independent data controllers** who determine their own purposes and means of processing. These parties may include:

- **Portfolio companies and investment vehicles**: Where necessary to maintain shareholder, investor, ownership, or other legally required records, administer investments, communicate with investors, or comply with applicable legal and regulatory obligations.
- **Co-investors, syndicate leads, founders, or other community participants**: Where necessary for a particular investment, networking, or community service, and where there is an appropriate legal basis. Where sharing is optional, we will provide the relevant choice or consent mechanism where required.
- **Professional advisers and service providers acting as independent controllers**: Such as legal, accounting, tax, financial, or other professional advisers where they determine their own processing purposes and means.
- **Regulators and public authorities**: Including financial-market regulators, tax authorities, law-enforcement bodies, courts, and other competent authorities where disclosure is required or permitted by applicable law.

Where a third party acts as an independent controller, that party is responsible for its own processing of personal data and may have its own privacy notice and data-protection obligations.

09

International Data Transfers (Focus: US Transfers)

Key Takeaway: Some of our service providers and business partners may process personal data outside the European Economic Area (EEA), including in the United States. Where this occurs, we take appropriate steps to ensure that international transfers comply with applicable data-protection laws and that appropriate safeguards are in place.

9.1 Why We Transfer Personal Data Internationally

We use third-party technology, infrastructure, communications, payment, community, analytics, and other service providers that may operate or process data in countries outside the EEA, including the United States.

International processing may be necessary to provide, maintain, secure, and improve our Platform and services. We seek to limit international transfers to information that is reasonably necessary for the relevant purpose.

9.2 Legal Framework

Where personal data is transferred outside the EEA, we rely on an appropriate legal transfer mechanism as required by applicable law. Depending on the recipient and circumstances, this may include:

- An **adequacy decision** adopted by the European Commission
- The **EU Standard Contractual Clauses (SCCs)** adopted by the European Commission, including the applicable 2021 modules
- The **EU–US Data Privacy Framework**, where the recipient is appropriately certified and the transfer is covered by the Framework
- Another lawful transfer mechanism or derogation recognized under applicable data-protection law.

Where SCCs or another mechanism requiring an assessment of the transfer is used, we consider the circumstances of the transfer and, where appropriate, conduct a **Transfer Impact Assessment (TIA)** and implement supplementary measures where necessary.

9.3 Supplementary Measures and Safeguards

Depending on the nature of the processing and the risks associated with the transfer, we may apply appropriate technical, contractual, and organizational safeguards, including:

Technical and Organizational Safeguards:
- Encryption of personal data in transit and, where appropriate, at rest
- Access controls and authentication measures
- Role-based access and least-privilege principles
- Multi-factor authentication where appropriate
- Data minimization and limitation of access to information necessary for the relevant service
- Pseudonymization or other privacy-enhancing measures where appropriate
- Security monitoring, logging, and incident-response procedures
- Appropriate backup, recovery, and business-continuity measures.

Contractual Safeguards:
- Data-processing agreements with relevant processors where required
- Appropriate confidentiality and security obligations
- Requirements concerning the use and protection of personal data
- Appropriate restrictions and safeguards concerning sub-processors
- Appropriate mechanisms for addressing government or law-enforcement requests for personal data, where required by applicable law.

Transfer Assessments:
We assess international transfers on a risk-based basis and may consider factors including the destination country's legal framework, the nature and sensitivity of the personal data, the purpose of the transfer, the recipient's technical and organizational measures, and the availability of supplementary safeguards.

Our international-transfer arrangements may change as our service providers, technology infrastructure, and applicable legal requirements change. We will update our safeguards and transfer mechanisms where reasonably necessary to maintain compliance with applicable data-protection requirements.

You may request further information about the safeguards applicable to a particular international transfer by contacting dpo@inovexus.com.

9.4 Your Data Location Preferences

Where available, Inovexus may provide options concerning the regional processing or storage of personal data. The availability and scope of these options depend on the Platform services you use, our technical infrastructure, and the capabilities of our service providers.

Standard Processing
- **Features**: Full Platform functionality
- **Data Location**: Personal data may be processed or stored in the EEA and, where necessary, in other countries including the United States
- **Processors**: Relevant approved processors and service providers as described in Section 8
- **International Transfers**: Protected using an applicable lawful transfer mechanism as described in Section 9.2

EU-Priority Processing
Where this option is available, we will seek to prioritize processing and storage within the EEA where technically and operationally feasible.

- **Data Location**: EEA preferred, with processing outside the EEA where necessary for a particular service or provider
- **Features**: Availability depends on the services and providers involved
- **International Transfers**: Any transfers outside the EEA remain subject to the safeguards described in this Section.

EU-Only Processing
An EU-only processing arrangement may be available for specific services, customers, or regulatory requirements where our infrastructure and service providers can support it.

An EU-only arrangement means that we will seek to restrict the relevant processing and storage of personal data to the EEA. However, this does not necessarily guarantee that no data will ever be accessed from or transferred outside the EEA, particularly where third-party services, support functions, or other technical dependencies are involved.

Any limitations, additional requirements, or costs associated with a particular data-location option will be communicated before the option is implemented.

To Request a Data Location Preference:
Email dpo@inovexus.com with the subject "**Data Location Preference**" and specify the option you would like to request.

We will assess the request and, where technically and legally feasible, implement the requested preference within **5 business days**. If the requested option is unavailable or cannot be fully implemented, we will explain the applicable limitations.

9.5 Transparency Regarding Government Requests

Inovexus and its service providers may receive requests for personal data from courts, regulators, law-enforcement agencies, or other public authorities.

Where we receive such a request, we will handle it in accordance with applicable law and will take reasonable steps to:

- Verify the validity and scope of the request
- Provide only the personal data that we are legally required or otherwise permitted to disclose
- Challenge or seek clarification of requests that we reasonably believe to be unlawful, excessive, or insufficiently justified, where legally and practically possible
- Maintain appropriate records of material requests and disclosures.

Where legally permitted and appropriate, we will notify affected individuals of a government or law-enforcement request. We will not provide such notification where prohibited by law or where doing so could prejudice an investigation, legal proceeding, or other legitimate legal interest.

Where appropriate and legally permissible, we may publish aggregated transparency information concerning government or law-enforcement requests. Such reporting will not identify individual users.

We do not guarantee that every government request will be challenged or that every affected individual will be notified, as these actions depend on applicable law, the circumstances of the request, and any restrictions imposed on us or our service providers.

9.6 Regular Review

We periodically review our international data-transfer arrangements and the safeguards applied to those transfers. Reviews may be conducted when appropriate based on:

- Changes in applicable data-protection laws or regulatory guidance
- Changes to the services, locations, or processing activities of our processors
- Changes in the nature or sensitivity of personal data being transferred
- Changes to applicable adequacy decisions or international-transfer mechanisms
- Significant security, technical, or legal developments.

Where necessary, we will update our transfer mechanisms, contractual arrangements, technical safeguards, or organizational measures to maintain compliance with applicable data-protection requirements.

Our internal compliance records may contain more detailed information about individual transfer assessments, processors, safeguards, and review dates. Such information may be made available where required by applicable law.

INOVEXUS

10

Data Retention and Deletion

10.1 General Principles

We retain personal data only as long as necessary to fulfil the purposes described above, or as required by law.

10.2 Retention Factors

Our retention periods consider:

- Legal and regulatory requirements
- Contractual obligations
- Business operational needs
- Data subject expectations and rights
- Risk management requirements

10.3 Retention Schedule

We retain personal data only for as long as reasonably necessary for the purposes for which it was collected, including to provide our services, maintain business and financial records, comply with legal and regulatory obligations, resolve disputes, enforce agreements, and establish or defend legal claims.

The retention periods below represent our **standard retention periods**. The actual retention period may vary depending on the nature of the information, the applicable legal or regulatory requirements, the status of an account or investment, and whether a legal hold or other lawful reason requires continued retention.

Data Category	Standard Retention Period	Typical Deletion / Review Trigger	Primary Basis / Purpose
Account Information	Account duration and, where necessary, for a period afterward to address legal, regulatory, security, or dispute-related requirements	Account closure followed by applicable retention review	Contract performance, legal claims, security, legal obligations
KYC / AML Documents	For the period required by applicable AML/CTF and financial regulations	Expiry of applicable statutory retention period and compliance review	Legal obligation
Investment Records	For the period required by applicable financial, commercial, tax, and regulatory requirements, which may be up to 10 years or longer where legally required	Expiry of applicable statutory or regulatory retention period	Legal obligation, legal claims
Tax Documents	For the period required by applicable tax laws	Expiry of applicable statutory retention period	Legal obligation
Communication Records	Generally for as long as necessary to manage the relationship, provide services, resolve disputes, and establish or defend legal claims	Periodic retention review based on the nature of the communication	Contract performance, legitimate interests, legal claims
Platform Usage / Analytics Data	Generally up to 24 months unless a longer period is reasonably necessary and lawful	Rolling deletion or anonymization	Legitimate interests, consent where applicable

Data Category	Standard Retention Period	Typical Deletion / Review Trigger	Primary Basis / Purpose
Marketing Preferences and Suppression Records	Retained as necessary to demonstrate and respect marketing preferences and opt-outs	Periodic review; suppression records may be retained where necessary to prevent unwanted communications	Legal obligation, legitimate interests
Event Data	Generally up to 2 years after the relevant event unless longer retention is reasonably necessary	Periodic retention review	Contract performance, legitimate interests, consent where applicable
Support Tickets	Generally up to 3 years after resolution, subject to the nature of the issue and any legal requirements	Periodic retention review following resolution	Contract performance, legitimate interests, legal claims
Startup / Investment Materials	For the duration of the relevant investment or business relationship and for an appropriate period afterward, subject to contractual, legal, and confidentiality requirements	End of applicable relationship and subsequent retention review	Contract performance, legal obligations, legal claims

Where different legal or contractual requirements apply to different categories of personal data, the **longer applicable retention requirement may prevail.**

Special Circumstances

Retention periods may be extended where reasonably necessary:

- **Legal Hold**: Where information is relevant to actual or anticipated litigation, arbitration, regulatory proceedings, investigations, audits, or other legal matters
- **Regulatory or Legal Requirement**: Where applicable law or a competent authority requires continued retention
- **Dispute Resolution**: Where information is reasonably necessary to establish, exercise, or defend legal claims
- **Security and Fraud Prevention**: Where limited information must be retained to prevent fraud, abuse, repeated account creation, or other security issues
- **Suppression Records**: Where limited information must be retained to ensure that a person who has opted out of marketing is not contacted again.

When personal data is no longer required, we will delete it, anonymize it, or otherwise securely dispose of it in accordance with our applicable policies and technical capabilities.

Deletion from active systems may not result in immediate deletion from all backups. Backup copies may remain for a limited period until they are securely overwritten or otherwise deleted through the normal backup lifecycle. Such copies will remain protected and will not ordinarily be restored or used except where necessary for disaster recovery, security, or legal purposes.

10.4 Deletion and Verification Process

We maintain procedures designed to ensure that personal data is deleted or anonymized when it is no longer required, subject to applicable legal, regulatory, contractual, and security requirements.

Our deletion processes may include:

1. **Retention Review**: Data is periodically assessed against the applicable retention period or deletion criteria.
2. **Legal Hold Check**: Where appropriate, information is checked against known litigation, regulatory investigations, disputes, or other circumstances requiring continued retention.
3. **Deletion or Anonymization**: Information that is no longer required is deleted or anonymized using appropriate technical and organizational measures.
4. **Processor Deletion**: Where applicable, we instruct relevant processors to delete or return personal data in accordance with our contractual arrangements and their applicable deletion procedures.
5. **Verification and Logging**: Appropriate records may be maintained to document deletion activities, exceptions, or legal holds.

We use security measures appropriate to the systems and storage technologies involved. These may include access controls, encryption, secure deletion mechanisms, logical deletion, cryptographic erasure, anonymization, and other appropriate technical measures.

We do not guarantee that every item of personal data can be physically or instantaneously removed from every backup, disaster-recovery copy, system log, or third-party system immediately upon expiry of a retention period. Where immediate deletion is not technically feasible, the information will remain appropriately protected and will be removed or anonymized in accordance with the relevant system's normal retention and deletion lifecycle.

We periodically review our retention and deletion practices to ensure that they remain appropriate for our services and applicable legal requirements.

INOVEXUS

11

Technical and Organizational Security Measures

We maintain technical and organizational measures designed to protect personal data against unauthorized access, accidental or unlawful destruction, loss, alteration, disclosure, or other forms of unauthorized processing.

The measures we apply are proportionate to the nature, scope, context, and risks of the processing and may include:

- Encryption of personal data in transit and, where appropriate, at rest
- Role-based access controls and least-privilege access
- Multi-factor authentication for administrative and privileged accounts
- Security monitoring and logging
- Vulnerability management, security updates, and patching
- Secure development and security-by-design principles
- Privacy-by-design and data-minimization practices
- Employee confidentiality obligations and appropriate security and privacy training
- Vendor due diligence and contractual security requirements
- Backup, recovery, and business-continuity measures
- Incident detection, response, investigation, and remediation procedures.

The specific security measures may vary depending on the system, service, type of data, and associated risk. We periodically review and update our security measures as appropriate.

11.1 Access Controls

We apply access controls designed to ensure that personal data is accessible only to authorized persons who require access for legitimate business, contractual, legal, or security purposes.

Our measures may include:

- **Principle of Least Privilege**: Access is limited to what is reasonably necessary for an individual's role and responsibilities.
- **Role-Based Access**: Permissions are assigned according to job function and responsibilities.
- **Multi-Factor Authentication**: MFA is required for administrative and other privileged accounts where supported and appropriate.
- **Access Reviews**: User permissions and privileged access are reviewed periodically based on risk and operational requirements.
- **Deprovisioning**: Access is removed or adjusted when personnel leave, change roles, or no longer require access.

11.2 Data Protection Measures

Depending on the system and sensitivity of the information, we may use:

- Encryption in transit and at rest
- Pseudonymization or other techniques to reduce unnecessary identification where appropriate
- Access restrictions and authentication controls
- Data classification and handling procedures
- Secure software-development and testing practices
- Vulnerability management and security updates
- Backup and recovery controls
- Logging and monitoring of relevant access and system activity.

We seek to apply appropriate technical safeguards to sensitive information, including financial, identity-verification, and other information requiring enhanced protection.

11.3 Monitoring and Incident Response

We maintain procedures for detecting, investigating, containing, and responding to suspected security incidents.

Depending on the nature of the environment and risk, these procedures may include:

1. **Detection**: Identification of potential security incidents through monitoring, system alerts, employee reports, processor notifications, or other sources.
2. **Containment**: Taking reasonable steps to limit unauthorized access, disclosure, alteration, or loss.
3. **Assessment**: Determining the nature and scope of the incident and identifying potentially affected systems and data.
4. **Investigation**: Assessing the cause, impact, and likelihood of harm to affected individuals.
5. **Remediation**: Taking reasonable measures to address the incident, restore affected services, and reduce the likelihood of recurrence.
6. **Documentation**: Maintaining appropriate records of incidents and the actions taken.

11.4 What Happens in a Data Breach

If we become aware of a personal-data breach, we will assess the incident promptly and take appropriate measures to contain, investigate, and remediate it.

Where required by applicable law, we will notify the relevant supervisory authority **without undue delay and, where feasible, within 72 hours after becoming aware of the breach**, where the breach is likely to result in a risk to the rights and freedoms of individuals.

Where a personal-data breach is likely to result in a high risk to the rights and freedoms of affected individuals, we will communicate the breach to those individuals without undue delay where required by applicable law.

Not every security incident or personal-data breach will require notification to individuals or a supervisory authority. The applicable notification requirements depend on the nature and severity of the incident and the risks involved.

Incident Response Process

Our response may include:

1. **Detection and Escalation**: Identify and escalate the suspected incident to the appropriate personnel.
2. **Containment**: Take reasonable steps to prevent further unauthorized access or disclosure.
3. **Risk Assessment**: Determine what personal data may have been affected and assess the potential risks to individuals.
4. **Regulatory Assessment**: Determine whether notification to a supervisory authority is legally required.
5. **Individual Notification**: Where legally required, notify affected individuals without undue delay.
6. **Remediation**: Address the underlying cause and implement appropriate corrective measures.
7. **Documentation**: Record the incident, assessment, decisions, notifications, and remediation measures as required.

Information Provided to Affected Individuals
Where notification to individuals is required, we will provide information appropriate to the circumstances, which may include:

- The nature of the personal-data breach
- The categories of personal data affected
- The likely consequences of the breach
- Measures taken or proposed to address the breach
- Measures individuals can take to protect themselves
- Contact information for obtaining further information or assistance.

Communication Channels
Depending on the circumstances and applicable legal requirements, notifications may be made through:

- Email
- Platform notifications
- Direct communication through another appropriate channel
- Website notices where appropriate for widespread incidents
- Other legally appropriate communication methods.

We maintain internal incident-response procedures and periodically review and test them based on the nature and risk of our processing activities.

Nothing in this section guarantees that a particular security measure, notification method, or response time will apply to every incident. Our response will depend on the circumstances of the incident and the requirements of applicable law.

INOVEXUS

12

Your Rights as a Data Subject

You have the following rights under the GDPR, subject to applicable legal limitations and exemptions:

- **Right of access** (Article 15): You may request access to your personal data and information about how we process it.
- **Right to rectification** (Article 16): You may request correction of inaccurate or incomplete personal data.
- Right to erasure (Article 17): You may request deletion of your personal data where the legal conditions for erasure are met.
- **Right to restriction of processing** (Article 18): You may request that we restrict the use of your personal data in certain circumstances.
- **Right to data portability** (Article 20): Where applicable, you may request certain personal data in a structured, commonly used, machine-readable format and request its transmission to another controller.
- **Right to object** (Article 21): You may object to processing based on legitimate interests. You have an unconditional right to object to processing of your personal data for direct marketing purposes.
- **Rights relating to automated decision-making** (Article 22): Where applicable, you have rights concerning decisions based solely on automated processing that produce legal effects or similarly significantly affect you.
- **Right to withdraw consent**: Where processing is based on consent, you may withdraw your consent at any time. Withdrawal does not affect the lawfulness of processing carried out before withdrawal.

How to Exercise Your Rights

You may exercise your rights by contacting:

- **Email**: dpo@inovexus.com
- **Postal address**: Inovexus, 4 Rue Royale, 75008 Paris, France

You do not need to use a specific form to exercise your rights.

We aim to respond to valid requests **within 15 days where reasonably possible**. In all cases, we will respond within the period required by applicable law. Under GDPR, **this is generally one month from receipt of the request**. Where permitted by law, this period may be extended by up to two additional months where a request is particularly complex or where we receive a large number of requests. If an extension is necessary, we will inform you of the reasons for the delay.

We may request additional information where reasonably necessary to verify your identity and protect personal data from unauthorized disclosure. We will seek to use proportionate verification measures and will not request identification documents unnecessarily.

Certain rights may be restricted where applicable law requires us to retain or process information, including information required for AML/CTF, tax, financial-regulatory, fraud-prevention, legal-claim, or other statutory purposes.

12.1 Right of Access — Article 15 GDPR

You may request confirmation of whether we process your personal data and, where applicable, obtain a copy of that data and information concerning:

- The purposes of processing
- The categories of personal data concerned
- The recipients or categories of recipients
- The expected retention period or the criteria used to determine it
- The source of the data where it was not collected directly from you
- Information about applicable automated decision-making and profiling
- Appropriate information about international transfers and applicable safeguards.

How to request:

1. Email dpo@inovexus.com.
2. Clearly state that you are making a data-access request.
3. Specify whether you want all personal data or particular categories of information.

Where appropriate, we may provide the information electronically in a commonly used format.

12.2 Right to Rectification — Article 16 GDPR

You may request correction of inaccurate personal data or completion of incomplete personal data.

For information that can be changed directly through the platform, you may update your profile or account settings.

For other information:

1. Email dpo@inovexus.com.
2. Identify the information you believe is inaccurate or incomplete.
3. Provide the corrected information and, where reasonably necessary, supporting documentation.

We will assess and correct information where appropriate. Information that must be maintained in an unchanged form for legal, regulatory, audit, evidentiary, or other lawful purposes may be retained, with appropriate contextual correction where necessary.

12.3 Right to Erasure — Article 17 GDPR

You may request deletion of your personal data where one of the grounds under Article 17 GDPR applies.

How to request:

1. Email dpo@inovexus.com with "**Deletion Request**" in the subject line.
2. Identify the account or personal data concerned.
3. Explain, where useful, the reason for your request.

We will assess the request and delete or anonymize personal data where legally required.

The right to erasure is **not absolute**. We may retain information where necessary to comply with legal or regulatory obligations, establish or defend legal claims, prevent fraud or abuse, maintain legally required records, or for another lawful exception under GDPR.

Where we have lawfully shared personal data with processors or other recipients, we will take appropriate steps to communicate an applicable erasure request where required by law and reasonably practicable.

12.4 Right to Data Portability — Article 20 GDPR

Where the right to portability applies, you may request personal data that:

- You have provided to us;
- Is processed by automated means; and
- Is processed on the basis of your consent or for performance of a contract.

Where applicable, we will provide the data in a structured, commonly used, and machine-readable format.

How to request:

- Email dpo@inovexus.com.
- State that you are making a data-portability request.
- Identify the information you would like transferred.

The portability right does not generally apply to data inferred or derived by us, such as internal scores, assessments, or proprietary analyses, unless otherwise required by applicable law.

12.5 Right to Object — Article 21 GDPR

You may object to processing based on our legitimate interests where you have grounds relating to your particular situation.

You may also object to the processing of your personal data for **direct marketing at any time and without having to provide a reason**.

Marketing objections:

- Click the unsubscribe link in our marketing emails; or
- Contact dpo@inovexus.com.

Marketing suppression requests will be processed promptly.

For other objections:

1. Email dpo@inovexus.com.
2. Identify the processing you object to.
3. Explain, where relevant, the reasons relating to your particular situation.

We will stop the relevant processing unless we can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or the processing is required for the establishment, exercise, or defense of legal claims.

12.6 Right to Restriction of Processing — Article 18 GDPR

You may request restriction of processing in circumstances provided by Article 18 GDPR, including where:

- You contest the accuracy of your personal data;
- Processing is unlawful but you prefer restriction rather than deletion;
- We no longer need the data but you require it for legal claims; or
- You have objected to processing and the applicable assessment is pending.

How to request:

Email dpo@inovexus.com and explain the circumstances supporting your request.

Where restriction applies, we will generally retain the relevant information but limit how it is processed, subject to the exceptions permitted by GDPR.

12.7 Rights Relating to Automated Decision-Making and Profiling

Where applicable, you may have rights under Article 22 GDPR in relation to decisions based **solely on automated processing** that produce legal effects or similarly significantly affect you.

Our AI systems may assist with recommendations, opportunity matching, prioritization, screening, and other platform functions. Where these systems are used only to provide recommendations or support human decision-making, they do not necessarily constitute automated decision-making within the meaning of Article 22.

Where an applicable Article 22 right arises, you may have the right to:

- Obtain appropriate information about the processing;
- Request human intervention;
- Express your point of view; and
- Contest the decision.

To request human review of an AI-supported outcome, contact dpo@inovexus.com with "**Human Review Request**" in the subject line and identify the recommendation or decision concerned.

We will assess the request and provide an appropriate response within the applicable GDPR timeframe.

12.8 Verification and Reasonable Requests

We may take reasonable steps to verify the identity of a person making a rights request where necessary to protect personal data from unauthorized disclosure.

We will generally use information already associated with your account where sufficient. Additional identification may be requested only where reasonably necessary and proportionate to the risk.

You will not normally be charged for exercising your GDPR rights. Where permitted by GDPR, we may charge a reasonable fee or refuse to act on requests that are manifestly unfounded or excessive, particularly because of their repetitive nature.

12.9 Complaints and Further Remedies

If you believe that we have not handled your personal data appropriately, you may first contact our DPO:

Email: dpo@inovexus.com
Postal address: Inovexus, 4 Rue Royale, 75008 Paris, France

You also have the right to lodge a complaint with a competent data protection supervisory authority.

For individuals in France, the relevant supervisory authority is the Commission Nationale de l'Informatique et des Libertés (CNIL).

You may also have the right to seek judicial remedies in accordance with applicable law.

INOVEXUS

13

Complete Cookie Policy

13.1 What Are Cookies?

Cookies are small text files or similar technologies stored on your device when you visit our website or use our platform. We may also use related technologies, including pixels, web beacons, SDKs, local storage, and similar identifiers.

These technologies may be used for security, authentication, functionality, analytics, service improvement, and marketing.

13.2 Strictly Necessary Cookies

Strictly necessary cookies are required for the website or platform to function securely and provide services you have requested. These cookies do not require consent where they are strictly necessary for the operation of the service.

Examples may include:

Cookie / Technology	Purpose	Typical Duration	Data Stored
session_token	Authentication and maintaining a secure login session	Session / as configured	Session identifier
csrf_token	Protection against cross-site request forgery and related attacks	Session / as configured	Security token
cookie_consent	Records your cookie and consent preferences	Up to 6 months (re-requested periodically per CNIL guidance)	Consent choices
Load-balancing technology	Helps route requests and maintain service availability	Session / as configured	Technical routing identifier

Legal basis: Where these technologies are strictly necessary, processing is based on the need to provide and secure the service and, where applicable, our legitimate interests in maintaining platform security and reliability.

These technologies cannot generally be disabled through our cookie preference mechanism because doing so may prevent the platform from operating correctly or securely.

13.3 Analytics Cookies and Similar Technologies

Where analytics technologies are not strictly necessary for the service, we use them only where the required consent has been obtained.

Depending on the services currently implemented, analytics technologies may include:

Service	Examples	Purpose	Types of Data
Google Analytics	_ga, _ga_*	Website usage, traffic measurement and service performance	Pages viewed, sessions, approximate device/ browser information, interactions
Hotjar	_hj*	User-experience analysis, heatmaps and session analysis	Clicks, scrolling, navigation and interaction patterns
Mixpanel	mp_*, distinct_id	Product analytics and feature-usage analysis	Feature interactions, navigation paths, events and conversion events

Analytics may help us understand:

- Which pages and platform features are used;
- Which features are adopted or underused;
- How users navigate through the platform;
- Where users encounter errors or usability problems;
- How long users interact with particular features;
- Which onboarding or platform steps are completed or abandoned;
- General platform performance and reliability;
- Aggregate engagement with community, event and investment-related features;
- The effectiveness of product improvements and communications where analytics are connected to those activities.

Where reasonably possible, we use aggregation, pseudonymisation, data minimisation and appropriate retention limits.

Legal basis: Consent (Article 6(1)(a) GDPR) where consent is required.

You may withdraw your consent at any time by contacting dpo@inovexus.com.

13.4 Functional and Preference Technologies

We may use technologies that remember choices you make, such as language, interface preferences, dashboard configuration or notification settings.

Examples may include:

Technology	Purpose	Typical Duration
language_pref	Remember language preferences	Up to 12 months
dashboard_layout	Remember dashboard or interface preferences	Up to 6 months
notification_settings	Remember notification preferences	Until changed

Where a technology is strictly necessary to provide a feature you have specifically requested, it may be used without consent where permitted by applicable law.

Where a technology is not strictly necessary, we will request consent where required.

13.5 Marketing and Advertising Technologies

With your consent where required, we may use advertising and marketing technologies to measure campaigns, understand advertising effectiveness, build audiences, or deliver more relevant communications and advertising.

Depending on the campaigns we run, these technologies may include:

Service	Examples	Purpose	Potential Data
LinkedIn Insight Tag	LinkedIn cookies/ identifiers	Measure LinkedIn campaign conversions and website interactions	Device/browser information, page visits, conversion events
Google Ads	_gcl_*, related Google identifiers	Measure advertising performance and, where enabled, remarketing/ audience measurement	Advertising identifiers, conversion events, website interactions
Meta Pixel	_fbp, _fbc	Measure Meta advertising performance and website conversions	Browser/device information, conversion events and advertising identifiers

These technologies may allow the relevant advertising provider to receive information about interactions with our website or campaigns.

Legal basis: Consent (Article 6(1)(a) GDPR) where required.

You may refuse or withdraw consent without affecting your ability to use the core platform.

Withdrawing marketing-cookie consent does not necessarily stop all marketing communications.
Email marketing preferences are managed separately through the unsubscribe mechanism in our emails or by contacting dpo@inovexus.com.

13.6 Third-Party Content and Embeds

Our website or platform may contain content or functionality provided by third parties, including:

- Video or media embeds;
- Social-media functionality;
- Scheduling or calendar tools;
- Maps and other interactive services;
- Payment or authentication components;
- Other third-party integrations.

Depending on how the integration operates, the third party may process technical information or place cookies or similar technologies on your device.

Where required, non-essential third-party technologies will be activated only after the relevant consent has been obtained.

Third-party providers may process information under their own privacy policies and terms.

13.7 Cookie Preference Management

Where consent is required, we provide a mechanism allowing you to make granular choices about non-essential cookies and similar technologies.

You may:

- Accept or reject non-essential cookie categories through our cookie-consent mechanism;
- Withdraw previously provided consent;
- Contact dpo@inovexus.com to request assistance with your preferences;
- Use your browser or device settings to manage or delete stored cookies;
- Use the unsubscribe mechanism included in marketing emails for email communications.

Your browser may allow you to block or delete cookies. However, blocking strictly necessary cookies may affect the availability or security of certain platform functions.

We may ask you to renew your consent where required by applicable law, including when the technologies or purposes materially change or when the applicable consent period expires.

13.8 Mobile Applications

Where we provide mobile applications, the applications may use technologies such as:

- **Device or advertising identifiers**: For analytics, security, attribution or advertising where permitted;
- **Push-notification tokens**: To deliver notifications where you have enabled them;
- **Local storage**: To remember settings and support application functionality;
- **Crash and diagnostic information**: To identify errors, improve reliability and maintain application security.

Where consent is required for analytics or personalised advertising, the relevant permission will be requested through the application or the applicable operating-system controls.

13.9 Email and Marketing Tracking

In addition to website cookies, our marketing communications may use technologies such as tracking pixels, unique links, or similar mechanisms to determine whether communications have been delivered, opened, clicked, or otherwise engaged with.

We may use this information to:

- Measure campaign performance
- Understand engagement with communications
- Improve the relevance and frequency of communications
- Maintain accurate communication preferences
- Identify inactive or outdated contacts
- Measure registrations or other actions resulting from communications.

Where consent is required for such tracking, we will obtain the appropriate consent. You may also opt out of marketing communications at any time using the unsubscribe mechanism provided in the communication or by contacting us at dpo@inovexus.com.

13.10 Browser Controls

Most web browsers allow you to control or delete cookies through their settings. You can generally:

- Block cookies
- Delete existing cookies
- Restrict third-party cookies
- Receive notifications before cookies are stored.

Browser controls may affect the functionality of our website or platform, particularly where strictly necessary cookies are involved.

13.11 Cookie Retention

Cookie lifetimes vary depending on their purpose and the technology involved. As a general benchmark, consent for non-essential cookies is treated as valid for approximately six months, in line with CNIL guidance, after which we will seek renewed consent.

Some cookies expire when you close your browser, while others may remain for a defined period or until you delete them or withdraw applicable consent.

We seek to configure non-essential cookies and similar technologies with retention periods appropriate to their purpose and to avoid retaining information for longer than necessary.

Where analytics or advertising information is linked to personal data held elsewhere, the applicable retention period may also be governed by our general data-retention policies.

13.12 Changes to This Cookie Policy

We may update this Cookie Policy when we introduce, remove, or materially change cookies or similar technologies, or where applicable legal or regulatory requirements change.

Where legally required, we will obtain renewed consent before activating newly introduced technologies that require consent.

Last updated: September 2026

INOVEXUS

14

Special Categories of Personal Data

We do not routinely seek to collect special categories of personal data under Article 9 GDPR.

Where such information is processed, we do so only where necessary and where an applicable legal condition under Article 9 GDPR is satisfied.

Examples may include:

Health and Accessibility Information

Where necessary for an event or service, we may process limited health or accessibility information, such as accessibility requirements or dietary information that may reveal health-related information.

Where required, this information will be processed on the basis of explicit consent or another applicable Article 9 condition.

We will limit the information collected to what is reasonably necessary for the relevant purpose and apply appropriate access controls and security measures.

PEP, Sanctions and Background Information

Information relating to politically exposed person (PEP) status, sanctions screening, adverse media, criminal-record information or other compliance checks may be processed for AML/CTF, financial-regulatory, fraud-prevention or related compliance purposes.

PEP status itself is not a special category of personal data under Article 9 GDPR. However, certain information obtained during compliance or background checks may fall under Article 9 or may be subject to other heightened legal protections.

Where criminal-offence or related data is processed, we do so only where permitted by applicable law and with the safeguards required by that law.

Access to compliance information is restricted to authorised personnel and service providers with a legitimate need to access it. Additional safeguards may include access controls, encryption, audit logging, segregation of sensitive information and restricted retention.

INOVEXUS

15

Data Protection for Minors

Our investment and membership services are intended for adults.

We do not knowingly provide investment services or adult membership accounts to persons under 18.

If we become aware that personal data has been collected from a person under 18 in circumstances where the collection was not permitted, we will take appropriate steps to delete the information and, where appropriate, close or restrict the associated account.

Where a particular service has different age requirements, those requirements will apply.

16

Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes to our services, technology, business practices or applicable legal and regulatory requirements.

Where changes are material, we will take reasonable steps to notify affected users, which may include email notification, a platform notice or another appropriate communication method.

Where the law requires renewed consent, we will obtain that consent before continuing the relevant processing.

The effective date and most recent update date will be displayed at the beginning or end of this Privacy Policy.

17

Complaint Rights

If you have concerns about how we process your personal data, we encourage you to contact us first so that we can investigate and, where appropriate, resolve the issue.

You may contact:

Data Protection Officer / Privacy Contact
Email: dpo@inovexus.com
Postal address: 4 Rue Royale, 75008 Paris, France

You also have the right to lodge a complaint with a competent data protection supervisory authority.

For individuals in France, the relevant supervisory authority is:

Commission Nationale de l'Informatique et des Libertés (CNIL)
Website: www.cnil.fr

If you are located in another EU/EEA country, you may also have the right to contact the supervisory authority in your country of residence, place of work, or the place where you believe an infringement occurred.

You may also have the right to seek judicial remedies in accordance with applicable law.

18

Final Provisions

18.1 Relationship to Terms of Service

This Privacy Policy supplements our Terms of Service and other applicable agreements governing use of the Inovexus platform.

Where there is a conflict between this Privacy Policy and another provision specifically concerning the processing or protection of personal data, the provisions of this Privacy Policy will apply to the extent required by applicable data-protection law.

18.2 Severability

If any provision of this Privacy Policy is determined to be invalid, unlawful, or unenforceable by a competent authority or court, that provision will be interpreted or modified to the extent necessary to make it lawful and enforceable where possible.

The remaining provisions will continue to apply to the fullest extent permitted by law.

18.3 Languages

This Privacy Policy is drafted in English.

Translations may be provided for convenience. Where a translation differs from the English version, the English version will prevail, except where applicable law requires otherwise.

18.4 Applicable Law and Jurisdiction

This Privacy Policy is governed by applicable French law and by the General Data Protection Regulation (EU) 2016/679 (GDPR), together with other applicable European and national data-protection legislation.

Any dispute concerning this Privacy Policy will be subject to the jurisdiction of the competent courts under applicable law.

Nothing in this section limits any mandatory rights you may have under applicable consumer, data-protection, or other laws, including any right to bring proceedings before the courts having jurisdiction under those laws.

18.5 Regular Review

We review this Privacy Policy periodically and at least annually, as well as when there are material changes to:

- The purposes or methods of processing;
- The categories of personal data processed;
- Our use of service providers or international transfers;
- Our AI or automated-processing activities;
- Applicable legal or regulatory requirements; or
- Our products, services, or platform architecture.

Next scheduled review: August 2027
The Privacy Policy will display its most recent update date.

18.6 Contact for Privacy Matters

For privacy questions, data-subject rights requests, complaints, or other matters concerning the processing of personal data, you may contact:

Data Protection Officer / Privacy Contact
Email: dpo@inovexus.com
Postal address: 4 Rue Royale, 75008 Paris, France

We do not publish a dedicated privacy telephone number. Where telephone contact is necessary, we will provide an appropriate contact method on request.

19

Version Control and Archive

19.1 Version History

We maintain records of previous versions of this Privacy Policy to document how our privacy practices have evolved and to support transparency and regulatory accountability.

Version	Date	Summary of Changes	Archive
7.1	August 31, 2026	Consolidated the duplicated Cookie Policy section into one, corrected a legal-citation reference, and aligned cookie-consent renewal with the CNIL ~6-month benchmark	Current
2.1	February 5, 2026	Enhanced international-transfer safeguards, retention framework, AI transparency and contestability procedures, and cookie-policy provisions	Archived internally
2.0	January 15, 2026	Major GDPR compliance revision, including expanded processing, rights, security, AI and international-transfer provisions	Archived internally
1.3	October 10, 2025	Added AI processing and international-transfer provisions	Archived internally
1.2	August 5, 2025	Enhanced cookie policy and processor information	Archived internally
1.1	June 1, 2025	Initial GDPR compliance version	Archived internally
1.0	May 15, 2025	First published version	Archived internally

Previous versions may be made available where appropriate and where doing so is necessary to demonstrate the privacy information applicable during a particular processing period.

19.2 Change Notification Process

We will communicate material changes to this Privacy Policy in an appropriate manner, taking into account the nature and significance of the change.

Where a change materially affects how we process personal data, we may notify affected users through one or more of the following:

- Email;
- Platform notification;
- Website notice; or
- Other appropriate communication channels.

Where applicable law requires renewed consent, we will obtain the required consent before carrying out the affected processing.

We will not treat continued use of the platform as consent where applicable law requires an affirmative consent mechanism.

Changes that are administrative, corrective, security-related, or otherwise non-material may be reflected through an updated version and effective date without advance individual notification where permitted by law.

19.3 Archive Access

We maintain previous versions of this Privacy Policy for appropriate historical, accountability, and regulatory purposes.

Where reasonably necessary, you may request a copy of the version of the Privacy Policy that applied to the processing of your personal data during a particular period by contacting:

dpo@inovexus.com

When making such a request, please identify the approximate period or date for which you require the historical version.

We may also provide relevant historical versions to competent supervisory authorities where legally required or reasonably necessary for regulatory purposes.

End of Privacy Policy

For questions regarding this Privacy Policy, your personal data, or the exercise of your GDPR rights, contact dpo@inovexus.com or write to:

Inovexus
4 Rue Royale
75008 Paris, France

INOVEXUS

APPENDIX A

Legal Basis Summary Table

The following table provides a high-level summary of the principal legal bases used for processing.
The applicable legal basis may vary depending on the specific service, relationship, jurisdiction, and circumstances of the processing.

Processing Activity	Data Categories	Primary Legal Basis (GDPR Art. 6)	Additional Basis / Context	Typical Retention
Account creation and management	Identity, contact information, account credentials	(b) Contract performance	(f) Legitimate interests for security and service protection	Account duration + applicable post-account period
KYC / AML verification	Identity, financial information, verification documents, compliance information	(c) Legal obligation	Applicable AML/CTF and financial-regulatory requirements	As required by applicable law
Investment processing	Identity, financial, transaction and contractual information	(b) Contract performance and (c) Legal obligation	Applicable financial, commercial and tax requirements	As required by applicable law
AI matching and recommendations	Profile information, investment preferences, professional information, relevant platform activity	(b) Contract performance and/or (f) Legitimate interests, depending on the specific processing	(a) Consent where required for optional profiling or non-essential processing	Account duration and/or applicable analytics period
Community platform	Profile, professional information, communications and community activity	(b) Contract performance	(f) Legitimate interests for security, moderation and service improvement; (a) Consent where required for optional visibility/sharing	Account duration + applicable post-account period
Marketing communications	Contact information, communication preferences and engagement information	(a) Consent where required	(f) Legitimate interests where permitted by applicable direct-marketing law	Until withdrawal or applicable suppression/ record-keeping period
Analytics and service improvement	Technical information, usage data, interaction data and aggregated/ pseudonymised information	(a) Consent where required for non-essential analytics	(f) Legitimate interests for strictly operational analytics where legally permitted	Typically up to 24 months, depending on purpose
Security and fraud prevention	Technical, account, authentication, transaction and other relevant information	(f) Legitimate interests	(c) Legal obligation where applicable	Varies according to incident, security and legal requirements
Tax reporting and compliance	Identity, financial and transaction information	(c) Legal obligation	Applicable tax legislation and reporting requirements	As required by applicable tax law
Event management	Contact, registration, attendance and event information	(b) Contract performance	(a) Consent for optional photography/media use or certain sensitive information where required	Typically limited to the period necessary for the event and related operational purposes

Processing Activity	Data Categories	Primary Legal Basis (GDPR Art. 6)	Additional Basis / Context	Typical Retention
Customer support	Contact information, account information and support communications	(b) Contract performance	(f) Legitimate interests for service quality, security and legal claims	Typically up to 3 years after resolution, subject to applicable requirements
Legal claims and dispute management	Relevant account, communication, transaction and other evidence	(f) Legitimate interests	(c) Legal obligation where applicable	For the duration of the relevant claim or applicable limitation/retention period

Key

- **(a) Consent**: Processing is based on your freely given, specific, informed and unambiguous consent where required.
- **(b) Contract performance**: Processing is necessary to enter into or perform a contract with you or to take steps at your request before entering into a contract.
- **(c) Legal obligation**: Processing is necessary to comply with a legal obligation applicable to Inovexus.
- **(f) Legitimate interests**: Processing is necessary for a legitimate interest pursued by Inovexus or a third party, provided that those interests are not overridden by your interests or fundamental rights and freedoms.

The legal basis identified in this table does not override any specific limitation, exemption, or additional requirement applicable to a particular processing activity.

INOVEXUS

APPENDIX B

Third-Party Processors

Our principal third-party processors are described in **Section 8.2 — External Processors of this Privacy Policy**.

Processors may engage approved sub-processors, including infrastructure, hosting, security, analytics, communication, payment, and other service providers necessary to provide their services.

We maintain appropriate contractual arrangements with processors and, where required, sub-processors, including data-processing agreements and applicable international-transfer safeguards.

Our processor-management practices include:

- Due diligence before engaging material processors;
- Appropriate data-processing agreements;
- Confidentiality and security obligations;
- Data minimisation requirements;
- Appropriate international-transfer mechanisms where required;
- Review of processor security and compliance measures;
- Management of sub-processor changes; and
- Periodic review of material processor relationships.

Where appropriate and legally required, we will inform users of material changes to relevant processors or sub-processors.

For questions regarding our processors or sub-processors, contact:

dpo@inovexus.com

INOVEXUS

APPENDIX C

Data Breach Notification

C.1 Internal Breach Classification

We maintain an internal incident-response framework for assessing and managing security incidents and personal-data breaches.

Incidents may be classified according to their nature, scope and potential impact, including:

Level 1 — Technical Incident: A security or technical incident where personal data is not affected or accessed.
Level 2 — Potential Personal-Data Incident: Personal data may have been accessed, altered, lost or disclosed, but the assessed risk to individuals is low.
Level 3 — High-Risk Personal-Data Breach: A personal-data breach presents a likely high risk to the rights and freedoms of affected individuals.
Level 4 — Major or Large-Scale Incident: A significant, large-scale or particularly sensitive breach requiring senior management, legal, regulatory and incident-response escalation.

The classification may be revised as additional information becomes available.

C.2 Notification to Supervisory Authorities

Where a personal-data breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the competent supervisory authority **without undue delay and, where required by Article 33 GDPR, within 72 hours after becoming aware of the breach**.

Where the breach is unlikely to result in a risk to individuals, notification to a supervisory authority may not be required.

Where notification is made after the 72-hour period, we will provide the reasons for the delay where required.

C.3 Notification to Affected Individuals

Where a personal-data breach is likely to result in a **high risk** to the rights and freedoms of affected individuals, we will notify those individuals **without undue delay**, unless an applicable GDPR exception applies.

Where appropriate, notification may include:

- The nature of the breach;
- The categories of personal data affected;
- The likely consequences;
- Measures taken or proposed to address the breach;
- Measures individuals can take to protect themselves; and
- Contact information for further assistance.

Notification may be provided by email, platform notification, postal communication, website notice, or another appropriate communication method depending on the circumstances and applicable law.

C.4 Incident Register

We maintain records of personal-data breaches and relevant security incidents as required by applicable law.

Records may include:

- Date and time of detection;
- Date and time the incident occurred, where known;
- Nature and circumstances of the incident;
- Categories and approximate number of affected individuals;
- Categories and approximate amount of personal data affected;
- Likely consequences;
- Containment and remediation measures;
- Risk assessment and decision-making;
- Notifications to supervisory authorities;
- Notifications to affected individuals; and
- Follow-up corrective measures.

C.5 Post-Incident Review

Material personal-data breaches are subject to a post-incident review appropriate to their severity.

Where appropriate, the review includes:

- Root-cause analysis;
- Assessment of existing technical and organisational controls;
- Corrective and preventive measures;
- Security-control improvements;
- Updates to policies and procedures;
- Additional staff training; and
- Verification that remediation measures have been implemented.

We regularly test and update our incident-response procedures to improve our ability to detect, contain, investigate and respond to security incidents and personal-data breaches.