PRIVACY POLICY

Thinking Globally Consulting Limited
Company Number: 17138834
Registered Office: 128 City Road, London EC1V 2NX, United Kingdom
Last Updated: 1 may 2026

1. INTRODUCTION

1.1 Who We Are

Thinking Globally Consulting Limited ("we", "us", "our", "the Company") is a strategic business and management consulting firm registered in England and Wales.

We provide non-regulated advisory services including:

- International corporate structuring and governance
- Crypto and blockchain business strategy with banking considerations
- Cross-border risk-aware architectures
- Contracts, documentation and business-level policies

1.2 Purpose of This Policy

This Privacy Policy explains how we collect, use, store and protect your personal data when you:

- Visit our website
- Contact us or request information about our services
- Engage us to provide consulting services
- Subscribe to our newsletters or communications
- Interact with us in any other way

1.3 Legal Basis

- We process personal data in accordance with:
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Other applicable UK data protection laws

1.4 Data Controller

Thinking Globally Consulting Limited is the data controller responsible for your personal data.

Contact Details:
Email: info@thinking-globally.com
Post: 128 City Road, London EC1V 2NX, United Kingdom

2. WHAT PERSONAL DATA WE COLLECT

2.1 Information You Provide to Us

When you engage with us, we may collect:

- Contact and Identification Data:
  - Full name
  - Job title and company name
  - Business email address
  - Telephone number
  - Postal address
  - LinkedIn profile or other professional social media (if provided)

Inquiry and Service Data:

- Information you provide in contact forms, emails or calls
- Details of services you are interested in or have purchased
- Project briefs, business information and materials you share with us
- Communications history (emails, meeting notes, call summaries)
- Feedback, survey responses and testimonials

Financial and Billing Data:

- Billing address and invoice contact details
- Payment references (we do not store full bank account or card details)
- Transaction records and payment history
- For clients using stablecoin payments: wallet addresses, transaction hashes (TxHash), blockchain network used, and related compliance information

Know Your Client (KYC) and Compliance Data.

Where required by law or our internal policies (particularly for clients making cryptoasset payments or operating in higher-risk sectors), we may collect:

- Copies of identification documents (passport, driving licence)
- Proof of address documents
- Company incorporation documents and registered office details
- Information about beneficial owners, directors and key decision-makers
- Source of funds and source of wealth documentation
- Sanctions screening results and risk assessment records

2.2 Information We Collect Automatically

Website Usage Data:

When you visit our website, we automatically collect:

- IP address
- Browser type and version
- Device type and operating system
- Pages visited, time spent on pages, referring URLs
- Date and time of access
- Cookies and similar technologies (see our Cookie Policy)

Technical and Security Data:

- Login data and access logs (if you use any password-protected areas)
- Security event logs (to protect against fraud and unauthorized access)

2.3 Information From Third Parties

We may receive personal data from:

- Introducers and referral partners who recommend our services
- Blockchain analytics providers (e.g., Chainalysis, Elliptic, TRM Labs) when screening cryptoasset payments
- Sanctions screening databases (e.g., HM Treasury, OFAC, UN, EU sanctions lists)
- Public sources such as Companies House, LinkedIn, company websites
- Professional advisers (legal, tax, accounting firms) where you have introduced us through them
- Email and productivity platforms (e.g., Google Workspace, Microsoft 365) used for project collaboration

3. HOW WE USE YOUR PERSONAL DATA

3.1 Lawful Bases for Processing

We process your personal data under one or more of the following lawful bases:

Purpose	Lawful Basis
Providing consulting services	Performance of contract
Responding to inquiries and quotes	Legitimate interests (business development)
Invoicing and payment processing	Performance of contract, Legal obligation (tax, accounting)
AML, sanctions and KYC compliance	Legal obligation (UK MLRs, POCA, sanctions law)
Marketing and newsletters	Consent (you can opt out anytime)
Improving website and user experience	Legitimate interests (service improvement)
Preventing fraud and security threats	Legitimate interests (security), Legal obligation
Legal claims and regulatory reporting	Legal obligation, Legitimate interests (protection of rights)

3.2 Specific Purposes

To Provide Our Services:

- Communicate with you about your project
- Deliver consulting services, analysis, reports and deliverables
- Manage project timelines, meetings and collaboration
- Coordinate with your team and any third-party advisers
- Provide ongoing advisory and retainer support

To Manage Payments:

- Issue invoices and track payment status
- Process payments (including stablecoin cryptoasset payments)
- Maintain payment records for accounting and tax purposes
- Handle any payment issues, shortfalls or overpayments

To Comply With Legal Obligations:

- Conduct Know Your Client (KYC) and customer due diligence (CDD)
- Screen clients, beneficial owners and transactions against sanctions lists
- Screen cryptoasset wallet addresses using blockchain analytics tools

- Identify and report suspicious activity to the National Crime Agency (SAR filings)
- Retain records for at least 5 years as required by UK anti-money laundering law
- Respond to lawful requests from regulators, law enforcement and tax authorities
- Comply with tax reporting obligations (e.g., DAC8, CARF for cryptoasset transactions)

To Protect Our Business:
- Enforce our Terms of Use and service agreements
- Defend legal claims and disputes
- Prevent fraud, money laundering and other financial crime
- Maintain information security and business continuity

To Improve Our Services and Website:
- Analyze website usage and user behavior
- Improve navigation, content and user experience
- Conduct internal research and service development

To Communicate With You:
- Send service-related emails (project updates, invoices, important notices)
- Respond to your inquiries and support requests
- Send marketing emails and newsletters (with your consent — you can opt out)
- Invite you to provide feedback or participate in surveys

4. WHO WE SHARE YOUR PERSONAL DATA WITH

We do not sell your personal data to third parties.

We may share your personal data with the following categories of recipients:

4.1 Service Providers and Subprocessors

IT and Communication Services:
- Email and productivity platforms (e.g., Google Workspace, Microsoft 365)
- Video conferencing tools (e.g., Zoom, Microsoft Teams, Google Meet)
- Project management and collaboration tools (e.g., Notion, Slack, Asana)
- Cloud storage and backup providers (e.g., Google Drive, Dropbox)
- Website hosting and content delivery networks

Payment and Compliance Providers:
- Payment processors for fiat and cryptoasset payments
- Blockchain analytics providers (e.g., Chainalysis, Elliptic, TRM Labs)
- Sanctions screening databases and AML compliance platforms

Professional Advisers:
- External legal, tax, accounting and regulatory advisers (where necessary for your project)
- Auditors and compliance consultants

4.2 Legal and Regulatory Authorities

We may disclose your personal data to:
- HM Revenue & Customs (HMRC) — for tax reporting and compliance
- National Crime Agency (NCA) — for suspicious activity reports (SARs) and financial crime investigations
- Financial Conduct Authority (FCA) — if required by regulation (we are not FCA-regulated but may be subject to ad hoc inquiries)
- HM Treasury / OFSI — for financial sanctions compliance
- Police, courts and tribunals — in response to lawful requests or legal proceedings
- Other competent authorities — as required by applicable law

4.3 Business Transfers

If we sell, merge, reorganize or transfer any part of our business, your personal data may be transferred to the new owner or successor entity, subject to confidentiality and data protection safeguards.

4.4 With Your Consent or Instructions

We may share your personal data with third parties where you have:
- Explicitly consented to the sharing, or
- Instructed us to coordinate with specific advisers, partners or stakeholders

5. INTERNATIONAL TRANSFERS OF PERSONAL DATA

5.1 Where We Store and Process Data

Your personal data is primarily stored and processed in the United Kingdom.

Some of our service providers (e.g., cloud hosting, email platforms, productivity tools) may store data in the European Economic Area (EEA), United States, or other jurisdictions.

5.2 Safeguards for International Transfers

Where we transfer personal data outside the UK or EEA, we ensure appropriate safeguards are in place:
- Adequacy decisions — transfers to countries recognized by the UK and/or EU as providing adequate data protection
- Standard Contractual Clauses (SCCs) — we use UK or EU-approved SCCs with our service providers

- Other approved mechanisms — such as Binding Corporate Rules or certification schemes where applicable

5.3 Further Information
If you would like more details about the safeguards we use for international transfers, please contact us at info@thinking-globally.com.

6. HOW LONG WE KEEP YOUR PERSONAL DATA

We retain personal data only for as long as necessary for the purposes set out in this Privacy Policy, or as required by law.

6.1 Retention Periods

Category	Retention Period	Legal Basis
General contact and inquiry data	Up to 3 years from last contact	Legitimate interests (business development)
Client project data and deliverables	6 years from end of engagement	UK tax and accounting requirements
Financial records (invoices, payments)	6 years from end of financial year	UK tax law
AML/KYC and compliance records	At least 5 years from end of business relationship	UK Money Laundering Regulations (MLRs)
Cryptoasset payment records (TxHash, wallet addresses, screening results)	At least 5 years from transaction date	UK MLRs, HMRC record-keeping
Suspicious Activity Reports (SARs) and related records	At least 5 years from SAR filing, or longer if investigation ongoing	POCA, Terrorism Act, NCA guidance
Marketing consent and communications	Until you withdraw consent, or 3 years from last engagement	PECR, legitimate interests
Website usage and analytics data	Up to 26 months (cookies), aggregated data may be kept indefinitely	Legitimate interests

6.2 Secure Deletion
When retention periods expire, we securely delete or anonymize personal data in accordance with our internal data retention and destruction policy.

6.3 Longer Retention in Special Cases
We may retain data for longer than the above periods where:

- Required by law or regulation
- Necessary to establish, exercise or defend legal claims
- You have provided explicit consent for longer retention

7. YOUR RIGHTS UNDER UK GDPR

You have the following rights regarding your personal data:

7.1 Right of Access (Subject Access Request)
You can request a copy of the personal data we hold about you.
How to exercise: Email info@thinking-globally.com with "Subject Access Request" in the subject line.
Response time: Within 1 month (may be extended to 3 months for complex requests).

7.2 Right to Rectification
You can ask us to correct inaccurate or incomplete personal data.

7.3 Right to Erasure ("Right to be Forgotten")
You can request deletion of your personal data where:

- It is no longer necessary for the purposes for which it was collected
- You withdraw consent (where consent was the lawful basis)
- You object to processing and there are no overriding legitimate grounds
- The data has been unlawfully processed
- Deletion is required to comply with a legal obligation

Limitations:
We may refuse erasure where we need to retain data to:

- Comply with legal obligations (e.g., AML record-keeping, tax law)
- Establish, exercise or defend legal claims

- Perform a task in the public interest or exercise official authority

7.4 Right to Restriction of Processing

You can ask us to restrict processing of your personal data where:

- You contest the accuracy of the data (pending verification)
- Processing is unlawful but you do not want erasure
- We no longer need the data but you need it for legal claims
- You have objected to processing (pending verification of legitimate grounds)

7.5 Right to Data Portability

Where processing is based on consent or contract and carried out by automated means, you can request a copy of your personal data in a structured, commonly used, machine-readable format (e.g., CSV, JSON).

7.6 Right to Object

To direct marketing: You can object at any time to processing for direct marketing purposes. We will stop immediately.

To legitimate interests processing: You can object to processing based on legitimate interests. We will stop unless we can demonstrate compelling legitimate grounds that override your interests, rights and freedoms.

7.7 Right to Withdraw Consent

Where processing is based on consent, you can withdraw consent at any time. Withdrawal does not affect the lawfulness of processing before withdrawal.

7.8 Right to Complain to the ICO

If you are unhappy with how we handle your personal data, you can lodge a complaint with the UK supervisory authority:

- Information Commissioner's Office (ICO)
- Website: https://ico.org.uk
- Telephone: 0303 123 1113
- Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

7.9 How to Exercise Your Rights

To exercise any of the above rights, please contact us at:

- Email: info@thinking-globally.com
- Post: 128 City Road, London EC1V 2NX, United Kingdom

We may request proof of identity to verify your request.

8. SECURITY OF YOUR PERSONAL DATA

8.1 Technical and Organizational Measures

We implement appropriate technical and organizational security measures to protect personal data against:

- Unauthorized or unlawful access, use, alteration or disclosure
- Accidental loss, destruction or damage
- Cyber-attacks, hacking and malware

8.2 Security Measures Include

- Access controls — role-based access, strong passwords, multi-factor authentication
- Encryption — data encrypted in transit (HTTPS, TLS) and at rest where appropriate
- Secure storage — cloud providers with ISO 27001 or equivalent certifications
- Regular backups — secure backup and disaster recovery procedures
- Staff training — all team members trained on data protection, confidentiality and information security
- Confidentiality obligations — employees and contractors bound by confidentiality agreements
- Incident response — procedures to detect, report and respond to data breaches

8.3 Data Breach Notification

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will:

- Notify the Information Commissioner's Office (ICO) within 72 hours where required
- Notify you without undue delay if the breach is likely to result in a high risk to you
- Take immediate steps to contain and remediate the breach

9. CRYPTOASSET PAYMENT-SPECIFIC DATA PROCESSING

9.1 Blockchain and On-Chain Data

Where you choose to pay us using stablecoins (USDT, USDC) or other cryptoassets:

Public Blockchain Records:

- Transactions are recorded on public blockchains (e.g., Ethereum, Tron)
- Transaction details (wallet addresses, amounts, timestamps, transaction hashes) are publicly visible and immutable
- We cannot delete or modify on-chain transaction data

Our Processing of On-Chain Data:

- We record wallet addresses (sending and receiving) and transaction hashes (TxHash) for compliance and accounting purposes
- We screen wallet addresses using blockchain analytics tools to assess AML, sanctions and financial crime risk
- We retain this data for at least 5 years as required by UK Money Laundering Regulations

9.2 Blockchain Analytics and Compliance Screening

Providers We Use:
- We use reputable blockchain analytics providers such as Chainalysis, Elliptic, TRM Labs or similar services.

What They Do:
These providers analyze on-chain transaction data and compare wallet addresses against:
- Sanctions lists (UK, EU, UN, US OFAC)
- Known links to darknet markets, ransomware, hacks, stolen funds
- Mixing/tumbling services and high-risk privacy protocols
- Other financial crime typologies

Risk Scoring:
- Analytics providers assign a risk score or rating (low/medium/high/severe) to wallet addresses and transactions.

Our Use of Screening Results:
- We review screening results before accepting cryptoasset payments
- High-risk transactions may be refused or returned
- We may file Suspicious Activity Reports (SARs) to the National Crime Agency where required by law
- Screening records are retained for compliance purposes

9.3 Your Rights Regarding On-Chain Data
Limitations on Erasure and Rectification:
- We cannot delete or modify data recorded on public blockchains
- We can delete or restrict our own internal records (off-chain) subject to legal retention requirements

Privacy-Enhancing Technologies:
If you use privacy protocols (e.g., RAILGUN, Fluidkey) with Private Proofs of Innocence or similar systems:
- We may accept payments from privacy-shielded addresses only if they pass our compliance checks
- We maintain records mapping customers to wallet addresses and transaction hashes as required by UK AML law
- Such records are securely stored and made available to UK law enforcement upon lawful request

10. COOKIES AND TRACKING TECHNOLOGIES

We use cookies and similar technologies on our website. For detailed information, please see our separate Cookie Policy.
Summary:
- Essential cookies: Required for website functionality (cannot be disabled)
- Analytics cookies: Help us understand website usage (Google Analytics or similar)
- Marketing cookies: Used for retargeting and ad campaigns (only with your consent)

You can manage cookie preferences through our cookie banner or your browser settings.

11. MARKETING AND COMMUNICATIONS

11.1 Marketing Emails and Newsletters
We may send you marketing communications (newsletters, service updates, promotional offers) where:
- You have given explicit consent (e.g., ticked an opt-in box), or
- You are an existing client and we are marketing similar services (soft opt-in under PECR)

11.2 Your Right to Opt Out
You can opt out of marketing communications at any time by:
- Clicking the "unsubscribe" link in any marketing email
- Emailing us at info@thinking-globally.com with "Unsubscribe" in the subject line
- Logging into your account (if applicable) and updating your preferences

What Happens After Opt-Out:
- We will stop sending marketing emails within 48 hours
- We may still send you service-related communications (invoices, project updates, important notices)

11.3 Third-Party Marketing
We do not sell or rent your email address to third parties for their marketing purposes.

12. CHILDREN'S PRIVACY

Our services are not directed at children under the age of 18. We do not knowingly collect personal data from children. If we become aware that we have collected personal data from a child without appropriate consent, we will take steps to delete that data promptly.
If you believe we have collected data from a child, please contact us immediately at info@thinking-globally.com.

13. LINKS TO THIRD-PARTY WEBSITES

Our website may contain links to external websites, platforms and services operated by third parties (e.g., LinkedIn, partner websites, regulatory resources).
We are not responsible for the privacy practices or content of third-party websites. We recommend you review their privacy policies before providing any personal data.

14. CHANGES TO THIS PRIVACY POLICY

14.1 Updates

We may update this Privacy Policy from time to time to reflect:

- Changes in our data processing practices
- New legal or regulatory requirements
- Feedback from regulators or best practice guidance
- Changes to our services or technology

14.2 Notification

When we make material changes, we will:

- Update the "Last Updated" date at the top of this policy
- Notify you by email (for significant changes affecting your rights)
- Display a notice on our website

14.3 Continued Use

Your continued use of our website or services after the updated Privacy Policy takes effect constitutes your acceptance of the changes.

If you do not agree with the updated policy, please stop using our services and contact us to discuss data deletion (subject to legal retention requirements).

15. CONTACT US

15.1 Data Protection Inquiries

If you have any questions, concerns or requests regarding this Privacy Policy or how we handle your personal data, please contact us at:

- Email: info@thinking-globally.com
- Post: Thinking Globally Consulting Limited
- 128 City Road, London EC1V 2NX, United Kingdom

15.2 Data Protection Officer

If you appoint a DPO, include their contact details here. For small consulting firms, a DPO is not mandatory unless you process special category data at scale or conduct systematic large-scale monitoring.

We aim to respond to all inquiries within 5 business days.

16. GOVERNING LAW

This Privacy Policy is governed by and construed in accordance with the laws of England and Wales.

Any disputes arising from this Privacy Policy shall be subject to the exclusive jurisdiction of the courts of England and Wales.

END OF PRIVACY POLICY

APPENDIX: LAWFUL BASES EXPLAINED

- Performance of Contract

Processing is necessary to fulfill our contract with you (e.g., to provide consulting services you have purchased).

- Legal Obligation

Processing is necessary to comply with UK or EU law (e.g., AML/KYC requirements, tax reporting, responding to court orders).

- Legitimate Interests

Processing is necessary for our legitimate business interests, provided these do not override your fundamental rights and freedoms. Examples include fraud prevention, business development, service improvement, and protecting our legal rights.

- Consent

You have given clear, affirmative consent for a specific purpose (e.g., marketing emails). You can withdraw consent at any time.

- Vital Interests

Processing is necessary to protect someone's life (rarely applicable in our business).

- Public Task

Processing is necessary to perform a task in the public interest or exercise official authority (not applicable to our business).

Document version: 1.0
Prepared for: Thinking Globally Consulting Limited
Jurisdiction: England and Wales (UK GDPR compliant)