Privacy Policy

Isadores.
Legal and Professional Services

1. Introduction

1.1 This Privacy Policy explains how Isadore Goldman Limited, a company registered in England and Wales with company number 08377344 whose registered office is at Suite 209, 2nd Floor, 75 King William Street, London, EC4N 7BE, ("**we**", "**us**", "**our**") collects, uses and shares personal data when delivering legal services, operating our website(s), administering our business, and using AI-enabled tools (including but not limited to the recording and transcription of telephone and video calls conducted via Microsoft Teams and Zoom) (together, the "**Services**"). It is issued in accordance with the UK General Data Protection Regulation ("**UK GDPR**"), the Data Protection Act 2018 ("**DPA 2018**") and the Data (Use and Access) Act 2025, which amends the UK's data protection and privacy framework. We are authorised and regulated by the Solicitors Regulation Authority ("**SRA**").

1.2 For the purposes of UK GDPR Articles 13 and 14, this is our privacy notice to clients, prospective clients, counterparties and their advisers, witnesses, experts, suppliers, event attendees, website users and other individuals about whom we process personal data (collectively, "**you**").

1.3 This policy supplements our engagement terms and any matter-specific notices. We may update it from time to time. The current version is displayed on our website and is available on request.

1.4 Our Services are intended for adults. We do not target children, but we may process children's data where necessary for a matter (for example, in family, tax, probate or safeguarding contexts).

2. How to contact us

2.1 Data Protection Officer

You can contact our Data Protection Officer, Sean Randall-Morris at:

Postal address: Suite 209, 2nd Floor, 75 King William Street, London, EC4N 7BE

Email: srandall@isadores.com

Telephone: 0800 208 8646

2.2 Complaints

If you have a concern or complaint about our handling of your personal data, please contact us using the details above. We will acknowledge your complaint within 30 days and investigate and respond without undue delay. We will keep you informed of the progress and outcome. You also have the right to complain to the UK Information Commissioner's Office ("**ICO**") at www.ico.org.uk at any time.

3. How we collect personal data

3.1 Direct interactions — You may provide data by phone, video call, email, post, in person at our offices, via secure portals, or when completing forms (including onboarding and identity verification).

3.2 Matter sources — We receive data from clients, counterparties, courts/tribunals, counsel, experts, witnesses, third-party platforms (e.g., disclosure or data-room tools), and insurers.

3.3 Public sources — We use publicly available sources and registers (e.g., Companies House, sanctions lists, credit reference agencies, media and professional directories).

3.4 Recordings and transcripts — In the ordinary course of business we record certain telephone calls and video conferences for the purposes set out in section 5 (including transcription and AI summarisation).

3.5 Website/technology — We collect technical and usage data from visits to our website(s) and systems and from communications we send (e.g., device identifiers, IP address, time stamps, and interaction data). See our Cookie Notice for details.

4. Categories of personal data we process

4.1 Identity and contact data — Names, former names, titles, roles, date of birth, contact details, identification numbers and copies of identification documents where appropriate.

4.2 Client/matter data — Information relating to your instructions or to a matter, including background facts, communications, documents and evidentiary material (which may include special category or criminal-offence data).

4.3 Financial and transaction data — Bank details, payment information, billing and collection data; source of funds/source of wealth information where required for AML purposes.

4.4 Technical and usage data — System and device identifiers, login data, IP address, browser type/version, time-zone settings, operating system and platform, and information on how you use our website, portals and communications.

4.5 Recorded data — Audio/video recordings of telephone calls and meetings, and associated transcripts/notes, including metadata (time, participants, meeting subject) where available.

4.6 Marketing and events data — Preferences, engagement with our briefings and events, dietary or access requirements you choose to provide.

4.7 Special category data — Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for identification, health data and data concerning sex life or sexual orientation, processed only where lawful and necessary (please see clause 6.6).

4.8 Criminal-offence data — Information about criminal convictions or allegations where relevant to a matter or required for legal/regulatory checks, processed under Article 10 UK GDPR and the DPA 2018 (please see clause 6.7).

5. AI-enabled tools and recording of calls/meetings

5.1 What we record — We may record certain inbound and outbound telephone calls and video conferences (for example on Microsoft Teams and Zoom) and generate automated transcripts and summaries. You will normally be notified at the start of a call/meeting where recording is enabled; for video calls a visual indicator may also be shown.

5.2 Purposes — (a) to capture and evidence instructions; (b) to aid accuracy, note-taking and quality assurance; (c) to produce attendance notes, action lists and file records; (d) to improve our workflows (e.g., search, categorisation and retrieval); (e) to manage risk and resolve complaints; and (f) to support training and mentoring within the firm (using anonymised or redacted content where reasonably possible).

5.3 Legal bases — We process recordings, transcripts and summaries where necessary for the performance of a contract with you or to take pre-contract steps (Article 6(1)(b) UK GDPR), and/or for our legitimate interests (Article 6(1)(f) UK GDPR) in documenting instructions, delivering and improving Services and managing risk. Where a legal obligation applies (e.g., compliance/quality records), we rely on Article 6(1)(c) UK GDPR.

5.4 Your choices — If you prefer not to be recorded, please tell your contact before or at the start of the call/meeting. We will offer reasonable alternatives (for example, disabling recording, using written channels, or scheduling a non-recorded call).

5.5 Vendor safeguards — We use reputable processors for transcription and AI summarisation under written contracts containing Article 28 UK GDPR terms. We configure tools so that your content is not used to train providers' general models. Data is encrypted in transit and at rest and access is restricted on a need-to-know basis.

5.6 Special category/criminal-offence data — Where recordings or transcripts contain special category data, we process them only when and to the extent that an Article 9 condition is met (typically Article 9(2)(f) UK GDPR: establishment, exercise or defence of legal claims, and/or substantial public interest under Article 9(2)(g) UK GDPR and/or the DPA 2018 Schedule 1 Part 2). For criminal-offence data we comply with Article 10 UK GDPR and applicable DPA 2018 Schedule 1 conditions (e.g., legal claims and regulatory requirements).

5.7 Automated decision-making — We do not currently make decisions based solely on automated processing, including profiling, that produce legal effects concerning you or similarly significantly affect you. If this changes, we will provide the information and safeguards required by applicable data protection law, including meaningful information about the processing and the opportunity to make representations, obtain human intervention and challenge a decision where those safeguards apply.

6. Purposes and lawful bases for processing

6.1 Providing legal services — To open files, perform conflict checks, take instructions, advise and represent clients, instruct counsel/experts, manage proceedings and deliver outcomes. Legal bases: performance of a contract or pre-contract steps (Article 6(1)(b) UK GDPR); legitimate interests (Article 6(1)(f) UK GDPR); legal obligations (Article 6(1)(c) UK GDPR). Special category data: Article 9(2)(f) UK GDPR legal claims and, where relevant, Article 9(2)(g) UK GDPR substantial public interest under the DPA 2018 Schedule 1. Criminal-offence data: Article 10 and DPA 2018 Schedule 1.

6.2 Firm administration — Practice management, billing and collection, supplier management, audits, responding to regulatory requests, ensuring security and business continuity. Legal bases: Article 6(1)(c) UK GDPR legal obligation; Article 6(1)(f) UK GDPR legitimate interests.

6.3 Compliance, AML and sanctions — Carrying out client due-diligence, source-of-funds/wealth checks and screening as required by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended). Legal bases: Article 6(1)(c) UK GDPR legal obligation; special category/criminal-offence data processed under the DPA 2018 Schedule 1 where applicable; retention per Regulation 40 (see 9).

6.4 Marketing and events — Sending legal updates, invitations and information about our Services; managing preferences and event administration (including dietary/access needs you choose to provide). Legal bases: Article 6(1)(f) UK GDPR legitimate interests or, where required by the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**"), consent (Article 6(1)(a) UK GDPR). You can opt out at any time.

6.5 Website/IT security and monitoring — Protecting our systems, detecting and investigating security incidents, monitoring email and systems use, preventing fraud and misuse. Legal bases: Article 6(1)(c) UK GDPR legal obligation; Article 6(1)(f) UK GDPR legitimate interests.

6.6 Special category data — We process special category data only where an Article 9 condition applies (commonly Article 9(2)(f) UK GDPR). Where we rely on substantial public interest, we satisfy the relevant condition(s) in Schedule 1 DPA 2018 and maintain an Appropriate Policy Document where required.

6.7 Criminal-offence data — Processed only under Article 10 UK GDPR together with a Schedule 1 DPA 2018 condition (for example, legal claims or regulatory requirements), and with appropriate safeguards.

7. Who we share your personal data with

7.1 We share personal data on a need-to-know basis with: (a) counsel, experts, mediators and other professionals we instruct; (b) courts/tribunals, law enforcement and regulators; (c) insurers and brokers; (d) service providers (IT, telephony, transcription/AI tools, data-room, disclosure/eDiscovery, secure messaging, document production, file storage and archiving); (e) banks and payment providers; and (f) event or webinar platforms and hosts. All processors are bound by contracts meeting Article 28 UK GDPR requirements.

7.2 Social media — We may use social media to publish firm news and events. If you engage with us on those platforms, your data are processed in accordance with each platform's privacy policy.

8. International transfers

8.1 We may transfer personal data outside the UK (and, where relevant, the EEA). Where we do so, we use one or more safeguards recognised by Chapter V UK GDPR: (a) UK adequacy regulations; (b) the UK International Data Transfer Agreement ("**IDTA**") or the UK Addendum to the EU Standard Contractual Clauses; and/or (c) another applicable derogation (for example, where the transfer is necessary for legal claims).

8.2 For transfers to the United States, we may in appropriate cases rely on the UK-US Data Bridge (the UK extension to the EU-US Data Privacy Framework) where the recipient is certified, or on the safeguards in 8.1(b). Before making a restricted transfer, we assess whether the UK GDPR transfer rules apply, identify an appropriate transfer mechanism and, where required, carry out and document the applicable data protection test or transfer risk assessment and adopt supplementary measures.

9. How long we keep personal data

9.1 We keep personal data only for as long as necessary for the purposes described in this policy, including to establish or defend legal claims, to comply with our professional and legal obligations and to maintain proper business records.

9.2 Matter files — Following termination of our retainer, we will maintain the electronic file for a period of six years from the date that matter is marked as closed. At the expiration of that six year period we shall confidentially destroy the electronic file within the following 12 month period without further notification to you. Information relating to Customer Due Diligence (e.g. verification of your identity, enhanced due diligence, and source of funds and wealth) will also be destroyed in the same timescale unless we have been retained by you on other matters that have been active more recently.

9.3 Marketing — We retain contact details for marketing until you opt out or we determine they are out of date, after which we will suppress or delete them.

9.4 Recordings/transcripts not linked to a matter — Where a recorded call/meeting does not proceed to an engagement, we usually retain the recording/transcript for up to two (2) years for quality assurance and risk management, unless a longer period is justified (e.g., a complaint or dispute).

10. Security of processing

10.1 We apply appropriate technical and organisational measures to protect personal data (Article 32 UK GDPR), including access controls, encryption, secure configuration, multi-factor authentication for remote access, staff training, supplier due-diligence and contractual safeguards, logging and monitoring, vulnerability management and tested backup/restore and business-continuity arrangements.

10.2 We operate incident-response procedures and will notify you and the ICO where required by law of personal data breaches that are likely to result in a risk to your rights and freedoms.

11. Your data protection rights

11.1 You have the following rights, subject to conditions and exemptions: to be informed; to access; to rectification; to erasure; to restriction; to data portability; and to object (including to direct marketing). You also have rights and safeguards in relation to significant decisions based solely on automated processing, including profiling, where applicable. We do not currently carry out such solely automated decision-making.

11.2 How to exercise your rights — Contact us using the details in section 2. We will respond without undue delay and within one month (extendable by two further months for complex requests). We may need to verify your identity and are permitted to charge a reasonable fee for manifestly unfounded or excessive requests.

11.3 Legal professional privilege — Where responding to a request would infringe legal professional privilege or confidentiality owed to others, we may withhold information to the extent permitted by law.

12. Marketing communications

12.1 We may send legal updates and invitations that are relevant to you. We rely on legitimate interests to do so, except where PECR requires consent. You can opt out at any time by using the unsubscribe link in our emails or by contacting us.

12.2 We may ask you periodically to confirm or update your marketing preferences, especially when you instruct us again or if laws change.

13. Third-party sites and links

13.1 Our website and communications may contain links to third-party sites and services. Those sites are not controlled by us and have their own privacy notices.

14. Changes to this policy

14.1 We may update this policy from time to time to reflect changes in law, guidance, technology or our processing practices. Material changes will be notified on our website and, where appropriate, directly to you.

15. Contact

15.1 Questions, requests or complaints about this policy or our handling of your personal data should be directed to our Data Protection Officer using the contact details in section 2.

ANNEX A
AI and transcription tools we use (overview)

A1. We may use the recording/transcription features of Microsoft Teams and Zoom and other contracted AI tools that create transcripts, extract action points and generate summaries. These tools are configured so that your data are not used to train providers' general models and are used under processor terms compliant with Article 28 UK GDPR.

A2. Outputs from AI tools are reviewed by lawyers or supervised legal professionals before reliance. We do not use AI to make decisions that produce legal or similarly significant effects without human review and input.

A3. If you would like a non-recorded channel, or a redacted/anonymised transcript for sharing, please tell your usual contact.

ANNEX B
Key legislation and guidance (non-exhaustive)

B1. UK GDPR (as incorporated by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019), in particular Articles 5, 6, 9, 10, 13–15, 17–22, 30, 32, 35 and Chapter V.

B2. Data Protection Act 2018, including Schedule 1 (special category and criminal-offence data conditions) and provisions on appropriate policy documents.

B3. Data (Use and Access) Act 2025, which amends the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

B4. Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) — rules on electronic marketing and cookies.

B5. Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended), including Regulation 40 on retention of records.

B6. SRA Standards and Regulations — confidentiality and information security obligations (where applicable).

B7. ICO guidance on AI and data protection, data protection impact assessments, international transfers, data protection complaints and marketing (www.ico.org.uk).