

Privacy policy

Belgium and United Kingdom | Updated 22 October 2026

Lina supports its clients with their legal needs through lawyers and a digital platform. This policy explains the processing that concerns visitors to [lina.law](#), users of the client portal [clients.lina.legal](#) and of the Lina OS lawyer portal on [lina.legal](#), as well as clients, prospects, people concerned by a matter, applicants and professional contacts. It also covers the Lina MCP connector and the lawyer portal on [lawyers.lina.legal](#) when that domain is in use.

“Lina” here means the entity concerned by the processing, not a single controller for all of the group’s activities. The entities’ contact details are given in the “Contact details” section. The European Union’s General Data Protection Regulation (GDPR), the applicable national laws and, where the processing falls within their scope, the UK GDPR and the Data Protection Act 2018 govern this processing.

Who is responsible for your data?

- Digital services, contact requests and commercial account management: Lina AI Ltd, whose contact details are given below, is the controller for the processing involved in operating them. Contracts with technical suppliers are entered into by this company.
- Legal matters: the lawyer or law firm named in your engagement letter determines the processing needed for its work, its professional obligations and the defence of the interests entrusted to it. Its contact details and professional information are provided to you before the engagement.
- Platform used on behalf of another firm: that firm remains the controller of the data in its own matters. To the extent that a Lina entity processes that data solely on its instructions, it acts as a processor under the applicable data processing agreement. Requests about the matter are then addressed to the firm, which Lina assists.

Lina AI SRL, established in Belgium, contributes to the technical development and support of the platform. Team members access data to the extent needed for their duties. For matter content processed on a firm’s instructions, the roles and obligations of each party are governed by the applicable data processing agreement; belonging to the Lina group does not confer a general right of access to matters.

1.What personal data does Lina collect and process?

We limit the information used to what is useful for the relationship or the matter concerned. Depending on the circumstances, it may include the following categories:

- Identity and contact details: surname, first name, business or personal contact details, job title, organisation, language of communication and contact information.
- Onboarding and due diligence: identity of the client, its representatives and beneficial owners, supporting documents and information needed for conflict checks, sanctions screening or anti-money laundering where those checks apply. A national number or a copy of an identity document is requested only where this is permitted and necessary.
- Legal matters: correspondence, contracts, deeds, evidence, financial, family or professional information and data about other parties, witnesses, advisers or participants. Health data or other special categories of data, as well as criminal offence data, may be needed for certain matters, under the conditions set out below.

- Accounts and usage: login, organisation, permissions, preferences, support requests, logins, IP address and technical events. Documents, instructions and results processed in a matter workspace may contain personal data.
- Billing and payments: billing identity, services, invoices, relevant bank details and payment status. Lina neither receives nor stores payment card data in the services described here.
- Communications and recruitment: subscriptions, preferences, correspondence, CVs and information provided in an application. Browsing and advertising: identifiers and interactions described in the cookie policy, according to your choices.

Source of the data

You may give us this information directly. We may also receive it from your employer, a client, another participant in the matter, an authority, a public register or a publicly available source, to the extent necessary for the engagement. Technical data comes from use of the services; connector data comes from the accounts connected by the lawyer. The forms include, in particular, opening a matter, messages to a lawyer and lawyer applications.

Where the information comes from a third party, we inform you within the applicable time limits, at the latest within one month or, if earlier, at our first communication with you or the first disclosure to another recipient. The exceptions provided by law, in particular those relating to professional secrecy, are assessed case by case.

2.How and on what basis does Lina use your personal data?

The table sets out the purposes and the legal bases relied on. The contractual basis concerns the person who is a party to the contract; for contacts at a client company or other people concerned by a matter, the processing relies on the stated legitimate interest or on an applicable legal obligation.

Purpose	Data and people concerned	Legal basis and interest pursued
Responding to a request, arranging a meeting or preparing a proposal	Identity, contact details and relevant information provided by the requester.	Pre-contractual steps requested by the person; otherwise legitimate interest in responding to business enquiries.
Advising, assisting and representing a client	Matter data relating to the client, its representatives and other participants.	Performance of the engagement for a client who is an individual; legitimate interest of the client and the firm in organising the advice, preserving rights and defending the interests at stake for other people.
Complying with professional, legal and tax obligations	Due diligence, conflicts of interest, supporting documents, invoices and filings.	Obligations applicable to the entity and the engagement, in particular professional rules, accounting, tax and anti-money laundering where the engagement is subject to it.
Providing and administering accounts and digital services	Contact details, access, support and data needed for the service.	Contract with the user who is an individual; legitimate interest in providing the service to the client organisation and managing its users' access. Content processed for another firm is subject to its instructions.
Protecting the services and handling incidents	Technical logs, access and information strictly needed for the incident.	Legitimate interest in preventing fraud, unlawful access and malfunctions; legal security obligations for the measures they require.
Sending news and promotional communications	Contact details and communication preferences.	Consent for subscriptions and mailings that require it. A statutory exception for marketing will be used only if its conditions are documented; a simple, free opt-out in every message.
Measuring audience and campaigns; personalising advertising	Browsing identifiers and events set out in the cookie policy.	Prior consent for optional audience or advertising trackers and uses. Refusal does not restrict access to essential features. Settings specific to Lina OS are set out in the cookie policy.
Reviewing applications and managing suppliers	CVs, correspondence, business contact details and contractual data.	Pre-contractual steps at the person's request; contract if they are a party to it; otherwise legitimate interest in recruiting and managing supplier relationships.
Establishing, exercising or defending Lina's own rights	Relevant information about a claim or dispute.	Legitimate interest in defending itself, limited to the information needed and subject to confidentiality obligations.

The bases above correspond to Article 6(1)(a), (b), (c) and (f) GDPR and to the corresponding provisions of UK law where they apply. We take account of people's rights and reasonable expectations for processing based on a legitimate interest.

Sensitive data, criminal offence data and minors

An Article 6 basis is not enough on its own for special categories of data. In a matter, processing them may in particular be necessary for the establishment, exercise or defence of legal claims (Article 9(2)(f) GDPR). Any other processing of such data must rely on a specific applicable condition. Data relating to criminal convictions and offences is subject to the authorisations and safeguards of the relevant national law; it is not processed on the basis of our legitimate interest alone.

The services are aimed mainly at professionals. A matter may nevertheless contain information about minors. It is processed only to the extent necessary for the engagement and with appropriate safeguards; the absence of accounts for minors does not therefore mean the absence of data about them.

Artificial intelligence tools

AI tools may assist with research, document analysis, document preparation and organising work. The data used remains subject to the purpose of the matter, to confidentiality and to the rules set out in this policy. Using AI is not a separate legal basis.

Anthropic Claude assists the Lina OS agents and the MCP connector; Google Gemini produces the numerical representations of documents needed for search (“embeddings”); Mistral OCR, used through Vertex AI in the Netherlands, extracts text from documents. Claude’s commercial terms and the terms of the paid Gemini service exclude the use of content to train or improve general models, subject to the optional sharing features and security processing provided for in those terms. No training does not mean no retention or no human security review at the providers. Agent sessions are stored at Anthropic; Lina does not benefit from a zero data retention arrangement.

Anthropic states that inputs and outputs of the standard API are deleted within 30 days, with exceptions for storage features, legal obligations and security. Persistent conversations follow their own deletion cycle. Google publishes a 55-day retention period for content subject to Gemini API abuse monitoring. These periods are not a single deletion deadline for the agent sessions, documents or embeddings kept in Lina matters; the schedule by category is given in section 7.

Lina does not take any decision based solely on automated processing that produces legal effects concerning you or similarly significantly affects you. Accepting or declining a client or a matter is a human decision; price estimates are reviewed before a quote is issued and every legal deliverable is reviewed by a lawyer. Advertising tools may build profiles for advertising purposes, with your marketing consent; those profiles do not decide whether your matter is taken on.

Connectors and applications chosen by the user

In Lina OS, lawyers connect the accounts they need for their work. Gmail is required in the current configuration and allows emails to be read, modified and sent. The Google Calendar and Microsoft Outlook connections are used to read the relevant emails or calendars. Depending on the permissions granted, Slack gives access to the messages and files in the workspaces available to the connected account, and Granola to the meeting notes and content available in that account. This data is used to find the context of a matter and to carry out the actions requested. The scope granted to each connection is shown when it is authorised.

You can revoke a connection from the security settings of the provider concerned and ask for its deletion at legal@lina.law. Access tokens are kept in the database until they are revoked, and must then be deleted together with any synchronisation copies that are no longer needed. Documents already added to a matter remain subject to that matter’s retention period; disconnecting does not delete them automatically.

The MCP connector can be used from Claude or ChatGPT. When a user enables it, the information needed for the requested actions and their results may be exchanged with the application they have chosen. How that application processes this information also depends on its user's contract, account type and settings. The fact that OpenAI is not a provider processing matters within Lina's infrastructure does not therefore mean there is no exchange with ChatGPT when a user chooses that application. Lina's commercial commitments to its own suppliers are not automatically those of the user's external account.

Required and optional information

The identity and contact details needed to respond to you, the information needed for the engagement and the billing information are required for the service concerned. The documents required by due diligence obligations are mandatory where those rules apply. Not providing them may prevent an engagement from being accepted or the service from being provided. The Gmail connection is required for the current use of Lina OS. Other information provided voluntarily, newsletter subscriptions and advertising choices are optional.

3. Who outside Lina may have access to your personal data?

Access within Lina is limited to the people who need it for their duties. Belonging to the group does not open general access to matters. Depending on the engagement or the service, recipients may include:

- The lawyers and staff working on the engagement; courts, arbitrators, mediators, experts, notaries, bailiffs, other parties and their advisers, where the work requires it and in compliance with professional secrecy and procedural rules.
- Hosting, storage, communication, support, security and AI providers, within the limits of their assignment. The services below are used by Lina AI Ltd; providers acting solely on its instructions must be covered by the applicable data processing agreements.
- Accountants, auditors, insurers, advisers and competent authorities, where a legal basis or the management of a right permits it. Reports under professional due diligence rules follow the procedures and restrictions specific to the profession.

Providers that use data for their own purposes must be identified as such. Their involvement does not automatically make them joint controllers with Lina; that classification depends on the processing actually organised.

The public website uses Google Analytics for audience measurement and Google Ads, Meta Pixel, OpenAI Ads and Ryze for advertising measurement and profiling, according to your choices. Intercom provides the chat, which is tied to the marketing choice in the current consent manager. The forms send conversion events without the content entered. The client portal has no audience or marketing tools. PostHog is limited to Lina OS: lawyers are identified, text and fields are masked and content properties are filtered. Optional usage analytics trackers are subject to consent. Any session replay requires specific prior consent, masking of matter content and retention of no more than 30 days.

The infrastructure uses Google Cloud for the APIs, Lina OS and documents in Belgium (eu-west-1), Supabase Pro for the database, authentication and files in Ireland (eu-west-1), Vertex AI for OCR in the Netherlands (eu-west-4), Neo4j AuraDB Free for the Lina OS graph in the United States (us-central1), and Vercel for the websites. Supabase's public DPA identifies Supabase Pte. Ltd in Singapore; Vercel's identifies Vercel Inc. in the United States. The server region and the provider's country are distinct. Linear receives the full content of requests; Slack the contacts; Gmail the emails sent; Intercom the conversations. The connections chosen by the lawyer may also involve Microsoft Outlook and Granola. Gemini processing is not guaranteed to take place exclusively in Europe.

4.Does Lina transfer your data outside the European Union?

Lina's international organisation and its use of certain providers may involve processing outside the European Economic Area (EEA) or the United Kingdom. Remote access from another country may also amount to a transfer. A server's European location alone does not therefore mean there are no transfers.

Transfers from the EEA to the United Kingdom may rely on the European Commission's adequacy decision in force, within its scope. For other countries, the safeguards required depend on the recipient and the applicable regime: the European standard contractual clauses and, where needed, the relevant UK mechanism, with the required assessment and supplementary measures. An adequacy decision or a certification can be relied on only for the recipients and processing it actually covers.

Processing	Known location	Safeguards and information
Intra-group services	Belgium and United Kingdom	Adequacy decision for EEA to United Kingdom flows within its scope; allocation of roles described in the introduction.
Google Cloud and Vertex OCR	Belgium and the Netherlands for the configured regions	Google's Cloud Data Processing Addendum sets out the processing rules and transfer mechanisms, including the standard clauses depending on the flows. Access from outside the region remains possible within the contractual limits.
Supabase Pro	Server in Ireland; provider Supabase Pte. Ltd in Singapore	Public DPA incorporated into the terms: European standard clauses and UK addendum. Choosing a region does not necessarily localise all support access.
Anthropic Claude agents	Processing outside the EU; sessions kept at the provider	Commercial DPA and standard clauses confirmed by the team. The public DPA also includes an addendum for transfers subject to the UK GDPR. Destinations depend on the services and sub-processors used.
Neo4j AuraDB Free	United States, us-central1	The Aura Self-Serve terms of 18 March 2026 incorporate the DPA. It provides for the Data Privacy Framework where applicable, the European standard clauses otherwise, and the UK addendum. The free tier is not, in principle, excluded from the DPA.
Paid Gemini API	Processing in the countries where Google or its providers have facilities	The Gemini terms refer to the Data Processing Addendum for Products where Google is a Data Processor. They do not guarantee exclusive European data residency.
Vercel	International infrastructure; provider in the United States.	The DPA provides for the European standard clauses and a UK addendum. The provider's address does not on its own determine where servers and access are located.
Communications, audience and advertising	Depending on the services and accounts used	Transfers outside the EEA or the United Kingdom may occur. The providers are identified in section 3 and in the cookie policy; the applicable safeguards depend on the service and the contract.

You can ask for information about these safeguards and obtain a relevant copy at legal@lina.law, subject to the redactions needed to protect confidential information. Your consent to cookies does not exempt Lina from complying with the transfer rules.

Documentation of the safeguards: cloud.google.com/terms/data-processing-addendum; supabase.com/legal/customer-resources/data-processing-addendum; anthropic.com/legal/data-processing-addendum; neo4j.com/legal-terms/data-processing-addendum; business.safety.google/processor/terms/; vercel.com/legal/dpa. You can ask for a copy of the safeguards that apply to your processing at legal@lina.law.

5. How does Lina protect your personal data?

The protection of matters relies on professional secrecy, access limited according to duties and confidentiality obligations. Technical and organisational measures must be suited to the sensitivity of the data and the risks of the services used.

Access to the portals is by invitation, through Google sign-in or a link sent by email. Data is encrypted in transit and at rest; technical secrets are managed in Google Secret Manager. Within Lina, operational access is limited to the internal team according to their duties. Supabase backups are kept for seven days. These measures are not a guarantee that no incident will occur.

Incidents are examined to determine their scope, the people concerned and the risks. Where a breach must be notified, the controller informs the competent authority without undue delay and, where feasible, within 72 hours of becoming aware of it; a high risk may also require the people concerned to be informed without undue delay. Where Lina acts as a processor, it informs the controller without undue delay. To send sensitive documents, use the channel agreed with your lawyer.

6. Your rights

Under the conditions set by the applicable law, you can ask for access to your data and for its rectification, erasure or the restriction of its processing. You can also receive the data you have provided in a structured format and transmit it to another controller where the right to data portability applies, in particular for automated processing based on contract or consent.

You can object, on grounds relating to your particular situation, to processing based on a legitimate interest. For direct marketing, your objection applies without any justification, including to profiling related to that marketing. You can withdraw your consent at any time; withdrawal does not affect the lawfulness of earlier processing. Cookie choices can be changed from the website's cookie manager.

The rights relating to decisions based solely on automated processing apply under the conditions of the regime concerned, in particular the safeguards of information, human intervention and the right to contest. In France, you can also give instructions about what happens to your data after your death, under the conditions set by law.

Send your request to legal@lina.law, which is read by the internal team concerned, stating the service or relationship it relates to. We respond without undue delay and, in principle, within one month. Any extension permitted by law is explained to you within that first period. The address already known to us is preferred for verifying your identity; a proportionate additional check may be needed in case of reasonable doubt. A copy of an identity document is not systematically required. Requests that require deletion at Linear, Slack, Intercom, Neo4j or Anthropic are followed up manually.

These rights are balanced against professional secrecy, the rights of other people and legal retention obligations. They do not give automatic access to another client's matter. Any restriction is assessed in light of its legal basis, and not merely because Lina carries out legal activities.

You can lodge a complaint with the competent supervisory authority without first having to obtain a favourable response from Lina or reach an amicable settlement. Depending on the processing and your situation, this may in particular be:

- Belgium: Data Protection Authority (APD/GBA), rue de la Presse 35, 1000 Brussels; www.autoriteprotectiondonnees.be.
- France: Commission nationale de l'informatique et des libertés (CNIL), 3 place de Fontenoy, TSA 80715, 75334 Paris Cedex 07; www.cnil.fr.
- United Kingdom: Information Commissioner's Office (ICO), Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF; ico.org.uk.

Within the EEA, you can in particular lodge a complaint with the authority of your habitual residence, your place of work or the place of the alleged infringement. These options do not exclude the court remedies available to you.

7.How long does Lina keep your personal data?

The schedule below sets out the retention periods and the deletion criteria adopted for each category. It distinguishes current use from limited archiving for a legal obligation or the defence of a right. Deletions may be manual. Data processed on behalf of a firm also follows its instructions and professional obligations. A period that applies to a document does not automatically extend that of the whole matter.

Category	Applicable period or criterion
Requests not taken further	3 years from the last active exchange about the request.
Legal matters	For the duration of the engagement and then, for lawyers' engagements governed by Belgian law, 5 years from their completion, subject to documents held in deposit, litigation and the specific obligations below. In England and Wales, the period is adjusted to the applicable claims, in particular the ordinary contractual limitation period of 6 years from when the cause of action arose; it does not follow automatically from the closing of the file.
Accounts	Duration of the relationship, then 3 months. Matter or billing documents subject to another retention ground follow their own schedule.
Email and calendar data from connections	Until the service concerned is disconnected; documents already placed in a matter follow that matter's schedule. Synchronisation copies and related indexes follow the deletion of their source where no other ground justifies keeping them.
Connector tokens	Until the authorisation is revoked; associated deletion of tokens and of synchronisation copies that are no longer needed.
Newsletter	Until unsubscription and, at most, 3 years from the last active contact. Merely sending a newsletter does not renew this period.
Applications	3 months after the end of the recruitment process; with separate consent, talent pool for 2 years from the last active contact.
Records of consent	13 months from the recording of the choice: choice, version, IP address, browser and date. This period differs from that of the cookie that stores the choice.
Technical logs	30 days from the event; only the elements needed to examine an incident may be set aside while it is handled and during the applicable remedy periods.
Supabase backups	7 days; this cycle does not guarantee the deletion of copies kept by other providers.
Cookies and local storage	Periods set out in the cookie policy, distinct from those of the data sent to providers.
Individual audience and usage analytics data	No more than 12 months after collection. Statistics that have been genuinely anonymised may be kept longer; merely replacing a name with an identifier is not enough.
Advertising measurement and attribution data	No more than 12 months after collection for individual data kept under Lina's control, subject to the rules specific to trackers on the device and to the evidence needed for a dispute. The platforms' own independent processing is also governed by their own notices.
Session replay, where specific consent has been given	No more than 30 days after recording, without matter content; only the elements needed to examine an incident may be set aside while it is handled.
Intercom conversations	Business enquiries not taken further: 3 years after the last active exchange. Technical support: 12 months after the request is resolved. Elements added to a legal matter follow that matter's schedule.

Category	Applicable period or criterion
Sessions and data at AI providers	Persistent sessions useful for a matter follow that matter's schedule; copies and interim results that are no longer useful are deleted when the task is closed. Deletion must also be requested from the providers concerned. Anthropic states 30 days for the standard API, excluding storage features, legal obligations and security exceptions. Persistent conversations have a separate cycle. The Gemini API provides for 55 days for content subject to abuse monitoring. Embeddings and extracts kept by Lina follow their source matter.
Accounting, tax and due diligence	Belgium: tax records relating to taxable income for the 10 years or financial years following the period concerned. United Kingdom: the company's accounting and tax records for 6 years after the end of the financial year concerned, unless extended by law. Where anti-money laundering obligations apply to the provider: in Belgium, identification documents for 10 years after the end of the relationship or the occasional transaction, and transaction records for 10 years after their execution; in the United Kingdom, in principle 5 years after the end of the relationship or the occasional transaction, subject to statutory exceptions.

Where litigation or a specific retention obligation justifies it, only the elements concerned are kept beyond the ordinary period, with restricted access, until the ground and the applicable time limits have ended. Backup retention follows a documented cycle; deleted data must not become active again when a backup is restored.

8.Changes to the privacy policy

We update this policy when the services, the processing or the applicable requirements change. The online version shows its date of update. Significant changes are notified by appropriate means; a new purpose is the subject of information and, where necessary, of the required consent before it is implemented. A change to the text does not, on its own, amount to consent to new processing.

Date of this version: 22 October 2026.

9.Contact details

For any question about your data or to exercise your rights, write to legal@lina.law. You can also send a letter to Lina AI Ltd or Lina AI SRL at the addresses below, marked "Data protection" and stating the service concerned. For a matter entrusted to a lawyer or a law firm, your request is directed to the controller of that matter.

Lina AI Ltd: company registered in England and Wales under number 17218368; registered office: 128 City Road, London EC1V 2NX, United Kingdom. Operator of the digital services and controller of the processing involved in operating them. Contact: legal@lina.law.

Lina AI SRL: Belgian private limited liability company (société à responsabilité limitée); company number: 1041.661.026; registered office: avenue Brugmann 198/2, 1050 Brussels (Ixelles), Belgium. Technical development and support of the platform. Shared contact: legal@lina.law.