PRIVACY STATEMENT THE LINQ GROUP B.V.

The Linq Group B.V., Danzigerkade 13-2, 1013 AP Amsterdam, the Netherlands

Registered with the Chamber of Commerce under number 70915792

Effective date: December 1, 2026. This version replaces all previous privacy statements of The Linq Group and LinqMaster.

1. Who we are and what this statement covers

The Linq Group B.V. (“The Linq Group”, “we” or “us”) operates the website www.linq.group and the online platform platform.linq.group (the “Platform”), including previous services offered under the LinqMaster name (www.linqmaster.app). Through the Platform we offer software and services for lead generation, outreach and lead management, including LinqMaster Seats, TLG Managed and Linq AI.

This privacy statement explains which personal data we collect, what we use it for and which rights you have. Unless indicated otherwise, capitalized terms have the same meaning as in our General Terms and Conditions (available via our website and the Platform).

We act in two different roles:

- Controller: for the personal data of visitors to our website, of Members who create an account, of contact persons of (prospective) clients and of recipients of our own marketing communications, we determine the purposes and means of the processing ourselves. That processing is covered by this privacy statement.
- Processor: the data our clients process within their Workspace, including prospect data and the content of conversations, is processed by us on behalf of the client. The client is the controller for that data. Our data processing agreement applies to that processing.

In addition, we manage a central enrichment layer of business company and contact data that we compile ourselves from public sources and license partners and that we manage across clients. We are the controller for this enrichment layer. We use this layer exclusively to supplement data within Workspaces and for aggregated or anonymized analyses; data imported by clients remains private to their Workspace.

2. Which personal data we process

Account data. When an account is created or a Member is invited, we process, among other things, first and last name, business email address, password (encrypted), role within the Workspace, language and country settings and, optionally, a profile picture.

Workspace and subscription data. Company name, address details, VAT number, selected products and terms, contract and billing data.

Payment data. Payments are handled by our payment provider Stripe. We receive payment statuses and invoice data; full card or bank details are processed by Stripe and are not stored by us.

Usage data. When you use the website and the Platform, we process technical data such as IP address, browser and device information, log files, date and time of use and usage statistics of functionalities.

Linked accounts and Channels. For outreach functionality, a Member with a Seat may link his or her LinkedIn account and one or more email accounts (for example Gmail, Microsoft 365/Outlook or IMAP) and, optionally, a calendar. Linking takes place via a secure connection flow that we operate with our infrastructure partner for Channels. Depending on the method, you log in directly with the provider (secure authorization), or your login details are used only to establish the connection and, where technically possible, are not stored afterwards. We store the access tokens needed to keep the connection active in encrypted form. Linking an account or providing login details is always voluntary. We use these links exclusively for the performance of the services, including sending and receiving messages and emails and showing conversations in the Inbox. A Member with a Seat can set their own Inbox in the platform to private at any time; conversations in an Inbox set to private are not visible to other Members or to employees of The Linq Group, except where technically necessary for the services or required by law.

Emails and tracking. When a Member sends emails via a linked mailbox, we process the content of those emails and any attachments, the sender and recipients, and replies and bounces. If tracking is switched on, we also register whether an email is opened and whether links in it are clicked. Addresses that unsubscribe or bounce are placed on the exclusion list of the Workspace.

Proposals and signatures. When a client sends a proposal via Linq Proposals, we process on behalf of that client the name and email address of the recipient, when and which pages of the proposal are viewed or downloaded and, upon signing, the typed name of the signatory, the time of signing, the email confirmation and a digital fingerprint (hash) of the signed document.

Communication data. Messages you exchange with us, including support requests, chat messages within the Platform and email correspondence.

Meeting and email data (TLG Managed). For our managed services we process emails and attachments that clients send us, notes of meetings and, where a meeting is recorded with our note-taking tool and this is announced, the transcript of that meeting.

Client Data (us as processor). Data that clients process within their Workspace about prospects and business contacts, including names, job titles, company information, contact details, public LinkedIn profile data, enrichment data and the content of outreach conversations. The client is the controller for this data; see section 10 of this statement. The data that a Member with a Seat builds up via their own linked Channel belongs first and foremost to that Member, as further set out in Article 34 of our General Terms and Conditions.

Marketing data. Data you leave via forms on our website, such as name, email address and company name, and your preferences for our newsletter and other communications.

3. What we use personal data for and on which legal basis

We process personal data for the following purposes, in each case on the legal basis under the GDPR stated with it:

- Providing the Platform and our services, including creating and managing accounts, Workspaces, Seats and Subscriptions (performance of the agreement).
- Invoicing and payment, including collection via Stripe (performance of the agreement and legal obligation).
- Providing support and communicating about the services (performance of the agreement and legitimate interest).
- Supporting our team with AI agents in delivering TLG Managed, including preparing replies, planning work and keeping a client dossier (performance of the agreement and legitimate interest).
- Taking notes of meetings with (prospective) clients, including recording and transcription where this is announced at the start of the meeting; you can object to recording at any time (legitimate interest).
- Securing, monitoring and improving the Platform, including analyzing aggregated usage statistics (legitimate interest).
- Sending newsletters, product updates and marketing communications; you can unsubscribe at any time via the unsubscribe link or by contacting us (consent and, for existing clients, legitimate interest).
- Complying with legal obligations, such as tax retention obligations (legal obligation).
- Establishing, exercising or defending legal claims (legitimate interest).

4. Linq AI

The Platform contains AI functionality (Linq AI), including the generation of draft messages, summaries, scores and the enrichment of lead and company data. For this functionality, the content required for it (such as conversation excerpts or company information) may be processed by carefully selected AI providers acting as sub-processors: Anthropic and OpenAI. We exclusively use their business APIs; these providers use the data only to deliver the requested output and not to train their models. Output of Linq AI may contain inaccuracies and is identified as AI-generated within the Platform where legally required. Within TLG Managed, our team is also supported by AI agents that,

among other things, prepare replies, plan work and keep a client dossier. These agents use the same AI providers and may process emails and attachments, meeting notes and transcripts that clients share with us. Messages that an agent prepares for third parties are only sent after approval by a person.

5. Who we share data with

We do not sell personal data. We only share personal data with service providers that help us deliver the services, and only in so far as necessary for that purpose. This concerns the following categories:

- Database and hosting services: Supabase, with our servers and database in Frankfurt, Germany.
- Application hosting: Vercel, with processing likewise primarily in Frankfurt, Germany.
- Payment provider: Stripe, for invoicing and payments.
- CRM and marketing services: HubSpot.
- Communication and email services: Microsoft.
- Secure browser environments for linked Channels: GoLogin.
- Infrastructure partners for linking and operating Channels (LinkedIn and email), with processing within the EU; these partners use network proxy partners solely to route encrypted traffic.
- AI providers for Linq AI functionality: Anthropic and OpenAI (via their business APIs; no training on client data).
- Runtime environment for AI agents: Railway.
- Error monitoring of the Platform: Sentry.
- Meeting notes and transcription: Fireflies.
- Document conversion when importing presentations into Linq Proposals: CloudConvert.
- Internal team communication and alerts: Slack.
- Data enrichment providers for supplementing business contact and company data.
- Other infrastructure partners for channel automation, contracted under data processing agreements.

An up-to-date overview of our sub-processors is available at: https://www.linq.group/data-verwerking-partners. In addition, we may share data with professional advisers, or where required by law, for example at the demand of a competent authority. In the event of a merger, acquisition or sale of assets, data may be part of the transaction; we will inform you before another privacy statement becomes applicable.

6. Transfers outside the EEA

We primarily process personal data within the European Economic Area (EEA). Some service providers, including certain AI and enrichment providers, may process data outside the EEA, including in the United States. In that case we ensure appropriate safeguards, such as an adequacy decision of the European Commission (including the EU-US Data Privacy Framework) or the European Standard Contractual Clauses, supplemented with additional measures where necessary. Our infrastructure partner for Channels uses some network proxy partners outside the EEA (including in the United States and Singapore) solely to route encrypted traffic to messaging platforms; these partners cannot read its content. Such transfers take place on the basis of the European Standard Contractual Clauses and a transfer impact assessment.

7. How long we retain data

- Account and Workspace data: for the duration of the agreement. After the end of the agreement, the client can export its data for another fourteen (14) days, after which we delete the data of the Workspace within thirty (30) days.
- Financial and tax data: seven (7) years on the basis of statutory retention obligations.
- Marketing data: until you unsubscribe or withdraw your consent.

- Usage data: aggregated or anonymized for internal analysis; no longer than necessary in identifiable form.
- Technical event logs of linked Channels (including message content received from channel providers): deleted automatically no later than ninety (90) days after receipt.
- Exclusion list (unsubscribes and bounces): for as long as the Workspace exists, so that an unsubscribe continues to be respected.
- Proposals and signed documents: for as long as the Workspace exists; signed agreements may be kept longer where necessary as evidence.

Data may be retained longer in so far as necessary to comply with a legal obligation or to establish, exercise or defend legal claims. Back-ups are overwritten according to a fixed schedule.

8. How we secure data

We take appropriate technical and organizational measures to protect personal data, including encryption of data in transit (TLS) and at rest (AES-256), separation of client environments (tenant isolation), role-based access rights, access logging and an internal access policy for our employees. However, no method of transmission or storage is completely secure; we cannot guarantee absolute security. If you suspect a security issue, please contact us immediately.

9. Cookies and website analytics

Our website and the Platform use functional cookies that are necessary for the operation of the service, such as session cookies for logging in. In addition, analytical and marketing tools may be used on our website to analyze the use of the website and to offer forms and content. Where legally required, we ask for your consent via the cookie settings on the website.

10. Have you been contacted by one of our clients?

Our clients use the Platform to reach out to business contacts, for example via LinkedIn or email. If you are contacted by one of our clients, that client is the controller for your data and we process it on behalf of that client. The data usually originates from public business sources (such as a public LinkedIn profile), from the client itself or from data enrichment providers. If you want to know which data a client processes about you, or if you want to object or have your data deleted, you can contact the client in question. You can also always contact us; we will then assist you and, where necessary, inform the client in question. If a client emails you via the Platform, that client may be able to see whether you open the email and click on links in it. Every commercial email contains an option to unsubscribe; once you unsubscribe, that client’s Workspace no longer emails you. If a client sends you a proposal via the Platform, the client can see when and which pages of the proposal you view.

11. Your rights

Under the GDPR you have the following rights with regard to your personal data:

- The right of access to the personal data we process about you.
- The right to rectification of inaccurate or incomplete data.
- The right to erasure (“right to be forgotten”).
- The right to restriction of processing.
- The right to object to processing, including to direct marketing.
- The right to data portability.
- The right to withdraw consent at any time.

You can exercise these rights by contacting us via the details at the bottom of this statement. We may ask you to verify your identity before we process a request. We will respond within one month; for complex requests this period may be extended by two months. If you disagree with how we handle your data, you have the right to lodge a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens, autoriteitpersoonsgegevens.nl) or the supervisory authority in your country of residence.

12. Minors

Our services are intended for business and professional use and are not directed at persons under the age of 18. We do not knowingly collect data from minors. If you believe that we are inadvertently processing data of a minor, please contact us and we will delete this data.

13. Automated decision-making

We do not make decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you. Scores and recommendations from Linq AI are tools for our clients and their users; there is always human involvement in decisions.

14. Changes to this privacy statement

We may update this privacy statement from time to time. The current version is always available on our website and in the Platform. In the event of material changes, we will inform you by email and/or a notification in the Platform before the change takes effect, and we will update the effective date at the top of this statement.

15. Contact

For questions about this privacy statement or to exercise your rights, you can contact us:

- Email: hello@linq.group
- Phone: +31 (0)20 209 1309
- Mail: The Linq Group B.V., Danzigerkade 13-2, 1013 AP Amsterdam, the Netherlands