

DATA PROCESSING AGREEMENT 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

Version: August 29, 2026. This version replaces all previous data processing agreements of The Linq Group and LinqMaster.

This data processing agreement applies as soon as the Client uses the Platform of The Linq Group B.V. and/or the services of The Linq Group, including TLG Managed. This data processing agreement forms an integral part of the Agreement and is accepted upon registration on the Platform or upon entering into the Commercial Contract. Capitalized terms not defined here have the meaning given to them in the General Terms and Conditions of The Linq Group.

Principles:

- The Linq Group offers an online SaaS service and additional services via the Platform, whereby the Client can enter, send, upload and have processed personal data of third parties within its Workspace;
- For this personal data, the Client determines the purposes and means of the processing. The Client is therefore the “Controller” and The Linq Group the “Processor” within the meaning of the GDPR;
- The Processor is willing to process the Personal Data under the responsibility of the Controller, and the Parties wish to record their rights and obligations in connection therewith.

The Controller and the Processor (jointly the “Parties” and each individually a “Party”) agree as follows:

Article 1. Definitions

GDPR the General Data Protection Regulation (Regulation (EU) 2016/679), including its national implementing legislation.

Data Subject the person to whom Personal Data relates.

Data Breach any breach of security leading accidentally or unlawfully to the destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, Personal Data processed.

Assignment all services provided by the Processor to the Controller, including making the Platform available and providing TLG Managed, whereby the Processor processes Personal Data for which the Controller is responsible within the meaning of the GDPR.

DPIA Data Protection Impact Assessment as referred to in the GDPR.

Personal Data any data relating to an identified or identifiable natural person that the Processor processes on behalf of the Controller in connection with the performance of the Assignment.

Sub-processor any party engaged by the Processor to process Personal Data for the purposes of the Assignment.

Workspace the Controller’s own online environment within the Platform.

Article 2. Data Subjects and categories of data

1. In performing the Assignment, the Processor processes Personal Data of the following categories of Data Subjects:
 - a) Members and employees of the Controller, including Linkers;
 - b) prospects and business contacts that the Controller manages or approaches via the Platform, including LinkedIn connections;
 - c) other persons whose data the Controller enters into or has processed in the Workspace.
2. The types of Personal Data processed under this data processing agreement include:
 - a) name and address details;
 - b) contact details, including telephone number and email address;

- c) business and professional data, including job title, employer and public LinkedIn profile data;
 - d) content of communications, including outreach messages and conversation history within linked Channels;
 - e) enrichment data added to contacts and companies;
 - f) account data of Members, including voluntarily provided login details for linked Channels;
 - g) usage and log data generated within the Workspace.
3. A further description of the processing operations is included in Annex 1.

Article 3. Performance of the processing

1. The Processor undertakes to perform the Assignment for the Controller under the conditions of this agreement and in accordance with the GDPR and/or other applicable laws and regulations.
2. The Controller has and retains full control over the Personal Data. The Processor processes the Personal Data exclusively on behalf of the Controller, on the basis of written instructions (including the instructions embodied in the use of the Platform and the Agreement), and not for its own purposes, except where required by law.
3. The Controller hereby grants the Processor general written authorization to engage Sub-processors for the processing. An up-to-date overview of Sub-processors is available at: <https://www.linq.group/data-verwerking-partners>. The Processor will inform the Controller of intended additions or replacements of Sub-processors, after which the Controller may object in writing on reasonable grounds within fourteen (14) days. If no reasonable alternative is available, the Controller may terminate the Agreement for the part concerned.
4. The Processor imposes on Sub-processors, by way of an agreement, the same or equivalent obligations as are imposed on the Processor in this agreement. The Processor remains responsible towards the Controller for the performance by Sub-processors.
5. Data that the Controller imports into or enters in the Workspace remains private to the Workspace and is not made available to other clients of the Processor. Enrichment data that the Processor adds from its own sources or from license partners (such as public company and job data) may be managed by the Processor, acting as controller for its own purposes, in its central enrichment layer and used in aggregated or anonymized form, in such a way that it cannot be traced back to the Controller or its Workspace.

Article 4. Rights of data subjects

1. Taking into account the nature of the processing, the Processor provides the Controller with reasonable assistance in fulfilling its obligation to respond to requests from Data Subjects (including access, rectification, erasure, restriction, objection and data portability). Where possible, the Platform facilitates these requests through self-service (including export and deletion functions).
2. At the Controller's first request, the Processor will, as soon as possible but no later than within five (5) working days, proceed to:
 - a) provide the necessary information;
 - b) correct, supplement, delete or block Personal Data; and
 - c) transfer Personal Data to the Controller or to a party designated by the Controller.
3. If a Data Subject contacts the Processor directly, the Processor will refer the Data Subject to the Controller and inform the Controller thereof, unless this is not permitted by law.

Article 5. Data Protection Impact Assessment

1. The Processor supports and provides reasonable assistance to the Controller in carrying out a DPIA and in any prior consultation of the supervisory authority.
2. The Processor supports and cooperates in the implementation of measures resulting from a DPIA or from changing laws and regulations.

3. The Processor will only charge reasonable costs actually incurred for this assistance.

Article 6. Security measures

1. Taking into account the state of the art and the nature of the processing, the Processor takes appropriate technical and organizational measures to secure the Personal Data against loss or any form of unlawful processing.
2. These measures include in any case:
 - a) encryption of data in transit (TLS) and at rest (AES-256);
 - b) logical separation of client environments (tenant isolation) within the Platform;
 - c) role-based access rights and user authentication;
 - d) an internal access policy for the Processor's employees, with access logging;
 - e) periodic back-ups that are overwritten according to a fixed schedule;
 - f) hosting of the production database within the European Union (Supabase, Frankfurt, Germany) and application hosting with processing primarily within the European Union (Vercel, Frankfurt, Germany).
3. The Processor warrants that persons acting under its authority are bound by confidentiality and only process the Personal Data lawfully and in accordance with this agreement.
4. The Processor informs the Controller without delay, and no later than within 24 hours of discovery, in detail of any Data Breach concerning the Personal Data. The Processor does not charge any costs for this and provides reasonable assistance with any notification obligation of the Controller towards the supervisory authority and Data Subjects.
5. Upon request, the Processor provides information about the measures taken to comply with the obligations under the GDPR and this agreement.

Article 7. Records

1. The Controller keeps a record of the processing operations for which it is responsible.
2. The Processor keeps a record of the categories of processing operations it carries out on behalf of the Controller, containing at least its name and contact details, the categories of processing and a general description of the security measures.

Article 8. Transfers of personal data

1. The Processor processes the Personal Data primarily within the European Union. The production database of the Platform is located within the European Union.
2. Transfers to countries outside the European Economic Area take place exclusively via Sub-processors and only if appropriate safeguards have been put in place as referred to in Chapter V of the GDPR, 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.
3. The current overview of Sub-processors states, for each Sub-processor, the processing location and the applicable safeguard.

Article 9. Confidentiality

1. All Personal Data processed by the Processor under this agreement is subject to a duty of confidentiality towards third parties. The Processor and all persons employed by or working for the Processor are obliged to keep the Personal Data confidential.
2. This duty of confidentiality does not apply in so far as this agreement provides otherwise, the processing is necessary for the Assignment, or a statutory provision or court decision requires disclosure.
3. The Processor informs the Controller immediately, and no later than within 24 hours of discovery, of any request from a third party for inspection or disclosure of Personal Data in violation of this duty of confidentiality.

Article 10. Term and termination

1. This agreement takes effect at the moment the Controller first uses the Platform or the services and agrees to the applicability of this agreement, and continues for as long as the Assignment continues.
2. This agreement ends by operation of law when the Assignment ends, without prejudice to the provisions that by their nature continue to apply, including confidentiality and liability.
3. The Parties may terminate this agreement with immediate effect by registered letter in the event of suspension of payments, bankruptcy or liquidation of the other Party.

Article 11. Return and deletion

1. The Controller can independently export its Personal Data via the Platform during the term of the Agreement and up to fourteen (14) days after its end. Upon request, the Processor provides reasonable assistance.
2. After expiry of the period referred to in paragraph 1, the Processor deletes all Personal Data of the Workspace completely within thirty (30) days, except in so far as a statutory retention obligation applies or retention is necessary to prove the performance of obligations. Personal Data in back-ups is overwritten in accordance with the fixed back-up schedule.
3. At the Controller's first request during the term, the Processor deletes specific Personal Data completely and irrevocably, subject to the exceptions referred to in paragraph 2.

Article 12. Liability

1. Each Party is responsible and liable for compliance with the obligations incumbent on it under the GDPR in its capacity as controller or processor respectively.
2. The liability of the Processor under or in connection with this agreement is subject to the limitations of liability set out in Article 12 of the General Terms and Conditions of The Linq Group, except in so far as mandatory law provides otherwise.

Article 13. Audits

1. The Controller is entitled to have compliance with this agreement audited no more than once a year by an independent, certified auditor, subject to a notice period of at least ten (10) working days and without unnecessary disruption of the Processor's business operations.
2. The Processor may also satisfy an audit request by providing a recent audit report or an equivalent statement from an independent, certified party.
3. The Controller bears the costs of the audit. If the audit reveals a material breach by the Processor, the reasonable costs of the audit will be borne by the Processor and the Processor will remedy the breach as soon as possible.

Article 14. Invalidity

If any provision of this agreement proves to be void or non-binding, the Parties remain bound by the remaining provisions. The Parties will replace the void or non-binding provision with a provision that is binding and whose purport corresponds as much as possible to that of the provision to be replaced, taking into account the purpose of this agreement.

Article 15. Miscellaneous

1. This agreement may be amended by The Linq Group in accordance with the amendment provisions in the General Terms and Conditions. The current version is always available via the website and the Platform.
2. In the event of a conflict between this agreement and the other arrangements between the Parties regarding the processing of Personal Data, this agreement prevails.

Article 16. Applicable law and choice of forum

1. This agreement and all non-contractual rights and obligations arising from it are governed by Dutch law.
2. All disputes arising in connection with this agreement will be settled by the competent court of the District Court of Amsterdam.

Annex 1. Overview of processing operations

Subject matter making the Platform available (including Workspaces, campaigns, sequences, Inbox, lead pipeline and Linq AI) and providing TLG Managed services.

Duration the term of the Agreement, plus the export and deletion periods of Article 11.

Nature and purpose hosting, storing, structuring, enriching, analyzing and transmitting data for the purposes of the Controller's lead generation, outreach and lead management, including sending and receiving messages via linked Channels and generating AI-assisted drafts and analyses.

Categories of Data Subjects Members and employees of the Controller (including Linkers); prospects and business contacts; other persons entered by the Controller.

Types of Personal Data name and address details; contact details; business and professional data (including public LinkedIn profile data); content of communications; enrichment data; account data and voluntarily provided login details for Channels; usage and log data.

Categories of Sub-processors database and hosting services: Supabase (Frankfurt, Germany) and Vercel (processing primarily Frankfurt, Germany); payment provider: Stripe; CRM and marketing services: HubSpot; communication and email services: Microsoft; secure browser environments: GoLogin; AI providers: Anthropic and OpenAI (via their business APIs, without training on client data); data enrichment providers; other infrastructure partners for channel automation. Current overview stating the processing location and safeguard for each Sub-processor: <https://www.linq.group/data-verwerking-partners>