LAST UPDATED: OCTOBER 22, 2026

Data Processing Agreement

This Data Processing Agreement (the "DPA") is between Groupshift Bilişim Teknolojileri ve Yazılım Hizmetleri Sanayi ve Ticaret Ltd. Şti. ("LyngL", "we") and the business that uses LyngL under the Terms of Service (the "Customer", "you"). It forms part of the Terms and applies whenever LyngL processes personal data on the Customer's behalf.

Download: Data Processing Agreement (PDF). If you need a signed copy, write to info@lyngl.com.

---

1. Definitions

- "Personal data", "processing", "data controller" and "data processor" have the meanings given in Law No. 6698 on the Protection of Personal Data ("KVKK") and, where it applies, the EU General Data Protection Regulation ("GDPR").
- "Customer Personal Data" means personal data that the Customer or its users put into LyngL, or that LyngL receives from services the Customer connects, and that LyngL processes on the Customer's behalf.
- "Sub-processor" means a third party that LyngL engages to process Customer Personal Data.
- "Security Page" means our Security and KVKK page.

2. Roles and scope

For Customer Personal Data, the Customer is the data controller and LyngL is the data processor. This DPA does not cover the personal data LyngL processes as a data controller, such as the Customer's account and billing details; our Privacy Policy covers those.

The subject, nature, purpose and duration of the processing, and the categories of personal data and data subjects, are described in Annex 1.

3. The Customer's instructions

LyngL processes Customer Personal Data only on the Customer's documented instructions. The Customer's use of LyngL (the goals it gives the Manager, the settings it chooses, the actions it approves and the services

it connects) and this DPA are its instructions. If LyngL believes an instruction infringes KVKK or the GDPR, it informs the Customer.

The Customer is responsible for having a lawful basis for the personal data it puts into LyngL, for informing data subjects and obtaining their consent where needed, and for putting special categories of personal data into LyngL only where it is necessary and lawful.

4. LyngL's obligations

LyngL:

- processes Customer Personal Data only to provide the service and as instructed, does not sell it and does not use it to train AI models;
- ensures that the staff who can access it are bound by confidentiality and access it only when necessary, for support, security or quality control, with each access logged;
- applies the technical and organisational measures in Annex 2 and keeps them at least at that level;
- helps the Customer, as far as reasonably possible, to respond to data subjects exercising their rights under Article 11 of KVKK or the GDPR, and with security, breach notifications and impact assessments;
- passes on to the Customer any request it receives directly from a data subject about Customer Personal Data and does not answer it itself unless the Customer authorises it;
- gives the Customer the information needed to show compliance with this DPA.

5. Sub-processors

The Customer authorises LyngL to use the sub-processors listed on the Security Page. LyngL imposes on each sub-processor data protection obligations that protect Customer Personal Data at least as well as this DPA, and remains responsible to the Customer for their performance.

LyngL announces a new sub-processor on the Security Page at least 15 days before it starts processing Customer Personal Data. Within that period the Customer may object in writing on reasonable data protection grounds. If the objection cannot be resolved, the Customer may end the affected part of the service and receive a pro rata refund of the fees it has prepaid for that part.

6. Transfers abroad

LyngL's sub-processors process Customer Personal Data outside Türkiye, in the locations listed on the Security Page. LyngL carries out these transfers in line with Article 9 of KVKK and, where the GDPR applies,

Chapter V of the GDPR, using the safeguards they provide for.

7. Security incidents

If LyngL becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, Customer Personal Data, it notifies the Customer without undue delay and at the latest within 72 hours, and gives the information the Customer reasonably needs to meet its own obligations, including notification to the Personal Data Protection Board.

LyngL takes reasonable steps to contain the breach and limit its effects, and keeps the Customer informed.

8. Audits

On request, LyngL answers written security questionnaires and provides documentation of the measures in Annex 2. Where this is not enough to show compliance, the Customer may, at most once a year and with 30 days' notice, have an audit carried out at its own cost by an independent auditor bound by confidentiality, during business hours and without disrupting the service or exposing other customers' data. Audits by a competent authority are not limited in this way.

9. Return and deletion

The Customer can export its content while its account is active, for example by downloading project files. When the Customer deletes a workspace or its account, or the Terms end, LyngL deletes the Customer Personal Data within 30 days, unless the law requires it to keep some of it.

Encrypted database backups are kept for at most 400 days and then deleted. Until then, deleted data in them is not used and stays protected as described in Annex 2.

10. Liability

Each party's liability under this DPA is subject to the limitations in the Terms, except where the law does not allow it to be limited.

11. Term, precedence and governing law

This DPA applies for as long as LyngL processes Customer Personal Data. Where it conflicts with the Terms on the protection of personal data, this DPA prevails. We may update it when the law or our service changes;

we publish the new version on this page with its date and tell Customers about significant changes in advance.

This DPA is governed by the laws of the Republic of Türkiye. The courts and enforcement offices of İzmir have jurisdiction over disputes.

12. Annex 1: Details of the processing

- Subject and purpose: providing LyngL, that is planning and carrying out the work the Customer requests with AI employees, such as research and reports, content, images and video, publishing, advertising, software and recurring jobs.
- Nature: collection, storage, organisation, retrieval, analysis, transmission to the providers a task needs, generation of new content, and deletion.
- Duration: while the Customer uses LyngL, plus the deletion periods in section 9.
- Data subjects: the Customer's users, and the people whose data the Customer puts into LyngL or LyngL receives from connected services, such as the Customer's customers, prospects, employees, candidates, suppliers and social media followers.
- Categories of personal data: identity and contact details, messages and emails, content and files, social media data such as usernames and comments, advertising results, and any other data the Customer chooses to put into LyngL.
- Special categories of personal data: only where the Customer puts them into LyngL, on its own lawful basis.

13. Annex 2: Technical and organisational measures

- Encryption in transit (TLS) for every connection; API keys and access tokens encrypted with AES-256-GCM; passwords stored only as one-way hashes; database backups encrypted with AES-256-GCM before they are stored; files encrypted at rest by the storage provider.
- Logical separation of each workspace's data, with every query scoped to its workspace.
- Access control: sign-in with Google or hashed passwords, secure session cookies, roles inside workspaces, and staff access limited to authorised persons, read-only and logged.
- Approvals for risky actions, hard ceilings on ad budgets and an emergency stop for all automation.
- An audit trail of tasks, tool calls, hand-offs, approvals and staff access.
- Rate limiting and abuse protection.
- Nightly encrypted backups kept for 14, 60 and 400 days, with tested restores.

- Choosing sub-processors with appropriate security commitments and limiting what each receives to what its role needs.

14. Annex 3: Sub-processors

The current list of sub-processors, with the role and location of each, is on our Security and KVKK page.