For B2B / agency customers who require GDPR Article 28 DPA. Status: Template — finalize with KVKK/GDPR counsel before signing.

This Data Processing Agreement ("DPA") supplements the Terms of Service between **Mesh Yazılım Teknoloji Limited Şirketi** ("Processor", "Nexus Dijital") and the entity identified below ("Controller").

By executing this DPA, the parties agree to the terms below for all Personal Data processed by Processor on behalf of Controller under the underlying Service Agreement.

---

1. Definitions

Terms used in this DPA have the meaning given in the **EU GDPR (Regulation 2016/679)**, the **UK GDPR**, and the **Turkish KVKK (Law 6698)** as applicable.

- **Personal Data:** any data the Processor processes in connection with the Service that identifies or relates to an identified or identifiable individual.
- **Processing:** any operation performed on Personal Data.
- **Sub-processor:** any third party engaged by Processor to process Personal Data on behalf of Controller.

2. Subject and duration

- **Subject:** Processor's processing of Personal Data on behalf of Controller in connection with providing the Nexus Dijital Service.
- **Duration:** Term of the underlying Service Agreement.
- **Nature & purpose:** content generation, scheduling, social media publishing, analytics, comment management, communication.
- **Types of Personal Data:** identity (name, email), contact (phone), professional (employer, role), usage logs (IP, timestamps), Controller-uploaded brand content, comments and DMs from end-user audiences.
- **Categories of data subjects:** Controller's employees and contractors, Controller's customers / leads, individuals whose data is contained in content posted via the Service, social media audience members.

3. Controller's obligations

Controller represents and warrants that: - It has a valid legal basis for the processing under applicable law. - It has provided required notices to data subjects. - Its instructions to Processor comply with applicable data protection law.

4. Processor's obligations

Processor will: - Process Personal Data only on documented instructions from Controller (the Service Agreement, the configuration in the Service, and any additional written instructions). - Ensure persons authorized to process Personal Data are bound by confidentiality. - Implement the technical and organizational measures in **Annex 2**. - Assist Controller in responding to data-subject rights requests. - Assist Controller with data-protection impact assessments and prior consultation where required. - Notify Controller without undue delay (and within **48 hours**) of any Personal Data breach. - Make available all information necessary to demonstrate compliance. - Allow for and contribute to audits, including inspections, conducted by Controller or a Controller-mandated auditor (subject to Section 9).

5. Sub-processors

- Controller authorizes Processor to engage the Sub-processors listed in **Annex 1**.
- Processor will inform Controller of any intended changes (addition or replacement) at least **30 days** in advance and provide an opportunity to object. If Controller reasonably objects, parties will work in good faith to resolve, including allowing Controller to terminate the affected service.
- Processor remains fully liable for Sub-processor obligations.

6. International transfers

- Where Personal Data is transferred outside Türkiye / EEA / UK, Processor implements appropriate safeguards: **Standard Contractual Clauses (SCC) Module 3** (Processor to Processor) where applicable, **UK IDTA** for UK transfers, and **KVKK Art. 9** mechanisms (binding undertaking or explicit consent) for cross-border KVKK transfers.
- Annex 1 lists Sub-processors and their locations.

7. Data subject rights

- Processor will, taking into account the nature of processing, assist Controller in fulfilling Controller's obligation to respond to data subject requests (access, rectification, erasure, restriction, portability, objection).
- Processor will forward to Controller any data subject request received directly that pertains to Controller's data, **within 5 business days** of receipt.

8. Personal Data breach

- Processor will notify Controller without undue delay and within **48 hours** of becoming aware of a Personal Data breach affecting Controller data.
- The notification will include: nature of breach, categories and approximate number of data subjects, likely consequences, measures taken or proposed, contact for further information.
- Processor will cooperate with Controller and provide information needed to fulfill Controller's obligations to notify supervisory authorities and data subjects.

9. Audits

- Once per 12-month period, Controller may audit Processor's compliance with this DPA at Controller's expense, with at least **30 days' written notice**, during business hours, in a manner that does not unreasonably disrupt Processor's operations.
- Processor may satisfy this obligation by providing an industry-standard third-party audit report (e.g., SOC 2 Type II) where available.
- Auditor must execute a confidentiality agreement.

10. Return / deletion

- On termination of the Service Agreement, Processor will, at Controller's choice, **delete** or **return** all Controller Personal Data within **30 days**.
- Backup copies are subject to Processor's standard retention (30 days) after which they are also deleted.
- Records that must be retained by law (tax, audit) are kept only for the legally required minimum and are deleted thereafter.

11. Liability

- Each party's liability under this DPA is governed by, and subject to the limitations of, the underlying Service Agreement.

12. Governing law and venue

- This DPA is governed by the law specified in the Service Agreement (Türkiye, İstanbul Çağlayan Courts).

13. Order of precedence

In the event of conflict between this DPA and the Service Agreement, this DPA prevails to the extent of the conflict in respect of data protection matters.

Annex 1 — Sub-processors

Sub-processor	Service	Location	Transfer mechanism
Ixnodes	Cloud infrastructure	Türkiye	Domestic (no transfer mechanism required)
Cloudflare, Inc.	CDN, DDoS, DNS	Global edge	SCC + UK IDTA
Anthropic PBC	AI text generation	US / EU	SCC
OpenAI, LLC	AI text + image	US / EU	SCC
Google LLC (Gemini API)	AI text	US / EU	SCC
fal.ai	AI image generation	US	SCC
iyzico Ödeme Hizmetleri A.Ş.	TR payment	TR	Domestic
Stripe Payments Europe Ltd.	Payment	IE/US	SCC
Resend, Inc.	Transactional email	EU	SCC

Up-to-date list and changes are published at https://nexusdijital.com/subprocessors. Controllers are notified via email of changes.

Annex 2 — Technical and organizational measures

Processor implements the following measures (non-exhaustive; see also our developer security docs):

A. Access control

- Role-Based Access Control across Workspaces and Brands
- WebAuthn (passkey) authentication; MFA required for paid plans
- Session lifetimes with idle / absolute timeouts

- Audit logging of admin actions; impersonation requires reason + ticket reference

B. Network security

- TLS 1.3 for all data in transit (external)
- Automatic mTLS between internal services (Linkerd)
- Default-deny firewall, Cloudflare WAF, rate limiting
- Segregated public and private network tiers; only the API gateway has a public IP

C. Data security

- Encryption at rest (full-disk encryption + envelope encryption for sensitive fields like OAuth tokens, MFA secrets)
- Row-Level Security (Postgres) for tenant isolation
- Per-service database role with schema-level privilege scope
- Encrypted backups; access restricted to SRE on rotation

D. Development security

- Continuous vulnerability scanning of dependencies and container images
- Cosign-signed images; ArgoCD verifies signatures on deploy
- CodeQL SAST on every PR
- Code review with two-reviewer approval for production branch
- Quarterly penetration testing after public launch

E. Operational security

- 24/7 on-call rotation; incident playbook; documented post-mortems
- Personnel security training on privacy and security
- Background checks where permitted by law for personnel with production access

F. Business continuity

- Daily encrypted backups; off-site copies
- Restore drills monthly
- Documented disaster recovery procedure

G. Privacy by design

- Data minimization in product flows
- Retention policies enforced by automated purge jobs
- Self-serve data export and deletion in the app