Data Processing Agreement (DPA) — Template

Version: 2026-04-19 (v1.0) **Issuing entity:** Sumatak Technologies LLP ("Processor", operating Gamyata) **Status:** Template — execute by signing the cover page and exchanging counter-signed copies with the Controller.

---

1. Parties

This Data Processing Agreement (the "DPA") is entered into between:

- **Controller:** *[Customer legal name, registered address, jurisdiction]*; represented by *[name, title]*; contact: *[data-protection contact email]*.
- **Processor: Sumatak Technologies LLP**, registered at *[Sumatak registered address, India]*, operating the Gamyata accessibility auditing platform; contact: `trust@gamyata.com` (and, for privacy matters, `privacy@gamyata.com`).

This DPA is incorporated into and forms part of the parties' Master Subscription Agreement, Order Form, or equivalent commercial agreement (the "Principal Agreement"). In the event of a conflict between this DPA and the Principal Agreement on matters of personal data processing, this DPA prevails.

2. Definitions

Capitalised terms not defined here have the meaning given to them in:

- **GDPR** — Regulation (EU) 2016/679;
- **UK GDPR** — the Data Protection Act 2018 read with the retained EU GDPR;
- **CCPA / CPRA** — Cal. Civ. Code §§ 1798.100–1798.199.100;
- **DPDP** — India's Digital Personal Data Protection Act, 2023.

"Personal Data", "Processing", "Controller", "Processor", "Sub-processor", "Data Subject", "Special Categories of Personal Data" carry their GDPR meaning. "Personal Information" carries its CCPA/CPRA meaning where the Controller's processing falls under that statute.

3. Subject Matter, Nature, Purpose & Duration

Item	Description
Subject matter	Provision of the Gamyata accessibility auditing service (scanning Controller-

Item	Description
	designated URLs, generating WCAG conformance reports, retaining issue tracking and remediation history).
Nature of processing	Storage, structured analysis, report generation, evidence retention, transmission to Controller users and authorised sub-processors.
Purpose	Performing the Principal Agreement; fulfilling Controller's accessibility-compliance obligations under ADA, EAA, Section 508, IS 17802 and equivalents.
Duration	Term of the Principal Agreement, plus retention periods set out in §11.

4. Categories of Data Subjects & Personal Data

Data subjects. The Controller's authorised users (administrators, auditors, developers, designers); end-users of Controller's tested websites *only* to the extent personal data appears in scanned page snapshots, screenshots, or DOM captures.

Personal data categories.

- *Account data:* name, work email, role, organisation, hashed password (handled via Logto), MFA factors, login telemetry.
- *Usage data:* scan submissions (URLs), report views, feature interactions, IP address (truncated for analytics, full for security logs), user-agent.
- *Billing data:* billing contact, billing address, GST/VAT ID; payment cardholder data is **not** stored by Processor — it is tokenised by Razorpay.
- *Scan content:* page HTML/CSS/JS captures, screenshots, accessibility findings. May incidentally include personal data exposed on the scanned page (names in copy, profile photos, comment threads). Controller represents it has lawful basis to submit such URLs.

Special categories. Processor does not solicit special categories of personal data. If they appear incidentally in scan content, both parties will minimise retention and Controller will instruct Processor to delete the affected scan on request.

5. Obligations of the Processor — GDPR Art. 28(3)(a)–(h)

In its capacity as Processor, Sumatak Technologies LLP shall:

1. **Process on documented instructions** — Process Personal Data only on the Controller's documented instructions, including with regard to transfers to a third country, unless required to do so by Union or Member State law to which Processor is subject.

2. **Confidentiality** — Ensure that personnel authorised to process the Personal Data are bound by written confidentiality obligations.

3. **Security measures** — Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including those described in Annex A (Technical and Organisational Measures).

4. **Sub-processors** — Engage sub-processors only under §6.

5. **Data subject rights** — Assist the Controller, by appropriate technical and organisational measures, in fulfilling its obligation to respond to requests for exercising the Data Subject's rights laid down in Chapter III GDPR.

6. **Security incident assistance** — Assist the Controller in ensuring compliance with Articles 32–36 GDPR (security, breach notification, DPIA, prior consultation), taking into account the nature of processing and information available to Processor.

7. **Return or deletion** — At the Controller's choice, return or delete all Personal Data after the end of the provision of services, unless Union or Member State law requires retention. Default: deletion within 60 days, with audit log retained for the period in §11.

8. **Audit cooperation** — Make available to the Controller all information necessary to demonstrate compliance with Article 28, and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, on the terms of §10.

6. Authorised Sub-Processors

The Controller authorises Processor to engage the following sub-processors as of the Effective Date. The current list is also published at https://gamyata.com/trust.

Sub-processor	Service	Region(s) of processing
Logto	Authentication & identity	EU
Amazon Web Services	Compute, storage, networking	ap-south-1 (Mumbai), eu-west-1 (Dublin)
Razorpay	Payment processing	India
Anthropic	Large-language-model inference for AI agents	United States (zero-retention agreement)
OpenAI	Large-language-model inference for AI agents	United States (zero-retention agreement)
Sentry	Error monitoring (PII scrubbing applied at ingest)	EU
PostHog	Product analytics (opt-in only)	EU

Processor will give the Controller at least 30 days' prior written notice of the addition or replacement of a sub-processor (via the trust page, release notes, or e-mail). The Controller may object on reasonable data-protection grounds within that notice period; if the parties cannot resolve the objection, the Controller may terminate the affected portion of the Principal Agreement.

Processor remains fully liable to the Controller for the acts and omissions of its sub-processors with respect to Personal Data.

7. International Transfers (Schrems II)

Transfers from the EU/EEA, UK, or Switzerland to India. The parties incorporate, by reference, the Standard Contractual Clauses adopted by the European Commission in Implementing Decision (EU) 2021/914 ("EU SCCs"), Module 2 (Controller-to-Processor), with:

- Clause 7 (docking clause) **enabled**;
- Clause 9, Option 2 (general written authorisation) for sub-processors, with a 30-day notice period;
- Clause 11 (independent dispute resolution) — left blank;
- Clause 17, Option 1 — governing law: Republic of Ireland;
- Clause 18 — supervisory authority: the Data Protection Commission of Ireland;
- Annex I.A populated from §1 above; Annex I.B from §3–§4; Annex I.C from Clause 18; Annex II from Annex A of this DPA; Annex III from §6.

Transfers from the UK are made under the UK International Data Transfer Addendum to the EU SCCs (issued by the ICO), with this DPA acting as the underlying agreement.

Transfers from Switzerland are made under the EU SCCs as adapted by the Federal Data Protection and Information Commissioner's guidance.

Schrems II supplementary measures. Processor implements the supplementary measures described in Annex A (encryption in transit and at rest, named-engineer access logging, government-access-request transparency) to ensure transferred data receives an essentially equivalent level of protection.

8. Personal Data Breach Notification

Processor shall notify the Controller of a Personal Data Breach affecting the Controller's Personal Data **without undue delay and in any event within 72 hours** of becoming aware of it. The notification will:

- describe the nature of the breach, including the categories and approximate number of data subjects and records concerned;
- communicate the contact details of the Processor's incident lead;
- describe the likely consequences and the measures taken or proposed to address the breach and mitigate its possible adverse effects.

If the full information is not yet available, the initial notification will identify what is known and Processor will provide updates as the investigation progresses.

9. Data Subject Requests

Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR (information, access, rectification, erasure, restriction, portability, objection, decisions based on automated processing).

If a data subject contacts Processor directly with such a request, Processor will, without undue delay, forward the request to the Controller and confirm to the data subject that the request has been forwarded.

10. Audit Rights

Once per twelve-month period, on at least 30 days' prior written notice, the Controller (or an independent auditor mandated by the Controller and agreed by the parties — agreement not unreasonably withheld) may audit Processor's compliance with this DPA. The audit:

- shall be conducted during normal business hours and in a manner that minimises disruption to Processor's operations;
- shall not require Processor to disclose information confidential to other customers;
- may be conducted remotely where appropriate evidence (SOC 2 / ISO 27001 reports, when available; security questionnaire responses; pen-test summaries) satisfies the Controller's requirements.

The Controller bears the costs of the audit unless it reveals a material breach of this DPA, in which case Processor bears the reasonable costs.

11. Return / Deletion of Personal Data

On termination of the Principal Agreement, or earlier on Controller's written request:

- Scan content, reports, and account data: **deleted within 60 days**.
- Audit and security logs containing Personal Data: retained for **12 months** for incident-response and legal-hold purposes, then deleted.
- Backups: deleted on the next backup-rotation cycle (maximum **35 days**).

On request, Processor will issue a written certificate of deletion.

If applicable Union, Member State, or Indian law requires Processor to retain specific Personal Data, Processor will inform the Controller of the retention requirement and the basis for it.

12. Liability

The liability of each party under or in connection with this DPA is subject to the liability cap and limitations set out in the Principal Agreement. Nothing in this DPA limits or excludes liability for (a) death or personal injury caused by negligence, (b) fraud or fraudulent misrepresentation, or (c) any other liability that cannot be limited or excluded by law.

13. Governing Law and Jurisdiction

This DPA is governed by the law specified in the Principal Agreement, except that the EU SCCs are governed as set out in §7. Disputes are subject to the jurisdiction agreed in the Principal Agreement, except that the EU SCCs supersede that choice for matters falling within their scope.

Annex A — Technical and Organisational Measures (TOMs)

A summary; current details live at https://gamyata.com/security.

- **Encryption in transit:** TLS 1.2+ for all external traffic; HSTS on all customer-facing endpoints.
- **Encryption at rest:** AES-256 for object storage and managed databases; AWS KMS-managed keys; per-tenant key separation roadmapped post-GA.
- **Access control:** SSO via Logto; role-based authorisation; MFA enforced for administrators; just-in-time access for production with audit log.
- **Network security:** VPC isolation; no public database endpoints; WAF on customer-facing surfaces; SSRF defence on URL ingestion.
- **Logging & monitoring:** centralised structured logs; PII scrubbed before ingest into Sentry; metrics in VictoriaMetrics; alerts route to on-call.
- **Vulnerability management:** Dependabot + container image scans on every build; quarterly third-party penetration tests planned post-GA; critical CVEs patched within 7 days.
- **Personnel:** confidentiality agreements; least-privilege access; background screening for production-access roles; annual security training.
- **Incident response:** documented runbook; named incident lead; 72-hour Controller notification commitment per §8.
- **Sub-processor governance:** §6; written contracts equivalent to this DPA.

Annex B — Cover Page (Signature)

Sumatak Technologies LLP — Authorised Signatory:

```
Name:       _____________________________________
Title:      _____________________________________
Date:       _____________________________________
Signature:  _____________________________________
```

Controller — Authorised Signatory:

```
Name:        _____________________________________
Title:       _____________________________________
Date:        _____________________________________
Signature:   _____________________________________
```

> **Compliance officer note (template only — flagged for legal-counsel review).** This DPA template is provided for buyer pre-procurement review and is not executed unless and until both parties sign Annex B. Specific clauses — particularly governing law, dispute resolution forum, liability cap reference, and the EU SCC modules — should be tailored per deal by Legal Counsel before execution. Items currently flagged for Legal Counsel review on first execution: §7 (SCC module annex completion), §10 (audit notice period for regulated-industry buyers), §12 (liability cap reference once Master Subscription Agreement is finalised).