GRAFT

GDPR TEMPLATE PACK

Data Processing Agreement (DPA)

Standard GDPR Data Processing Agreement between Graft (processor) and a client (controller). Covers sub-processors, security measures, breach notification, audit rights and cross-border transfers.

VERSION	LAST UPDATED	PUBLISHED BY
v1.0	**2026-04-07**	**Graft**

TEMPLATE — REQUIRES LEGAL REVIEW BEFORE USE

This document is a drafting aid. Your DPO, legal counsel or works council should review every section before use.

> **WARNING**
> **Template -- requires legal review.** This is a starting point for the DPA between Graft and a client. Both parties' legal counsel should review and negotiate specific terms, commercial caps, and jurisdictional variations before signature.

1. Parties

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

Controller `<<CLIENT FIELD: Client legal entity name>>` `<<CLIENT FIELD: Registered address>>` represented by `<<CLIENT FIELD: signatory name, role>>` ("the Controller")

and

Processor Graft Ltd `<<GRAFT REGISTERED ADDRESS>>` Company number: `<<GRAFT COMPANY NUMBER>>` represented by a director of Graft Ltd ("the Processor" or "Graft")

together "the Parties".

2. Scope and purpose

This DPA governs the Processor's processing of personal data on behalf of the Controller in connection with the Controller's use of the Graft hybrid workflow assessment service ("the Service"), as described in Schedule 1.

This DPA is entered into pursuant to Art. 28 GDPR and forms part of the principal services agreement between the Parties ("the Principal Agreement"). In case of conflict between this DPA and the Principal Agreement in matters relating to the processing of personal data, this DPA prevails.

3. Definitions

Terms not otherwise defined in this DPA have the meanings given to them in Regulation (EU) 2016/679 ("GDPR") and in the Data Protection Act 2018 where applicable in the United Kingdom.

For the purpose of this DPA:

- **"Personal Data"** means any personal data processed by the Processor on behalf of the Controller under this DPA, as described in Schedule 1.
- **"Sub-processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller, as listed in Schedule 3.
- **"Data Subject Request"** means any request by a data subject to exercise their rights under Chapter III GDPR.
- **"Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

4. Processing on documented instructions

4.1 Instruction framework

The Processor shall process Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a third country or international organisation, unless required to do so by Union or Member State law. The Principal Agreement, this DPA, and the Controller's use of the Service constitute the Controller's documented instructions.

4.2 Prohibited uses

The Processor shall **not**, for any reason:

- Produce individual-level performance, productivity, or disciplinary reports from the Personal Data processed under this DPA;
- Use the Personal Data to train generative AI models for the benefit of any third party;
- Sell, rent or disclose the Personal Data to any party not listed in Schedule 3;
- Re-identify any data subject from aggregated outputs.

4.3 Legal conflict notification

If the Processor believes that an instruction from the Controller infringes the GDPR or other applicable data protection law, it shall inform the Controller immediately.

5. Confidentiality

The Processor shall ensure that personnel authorised to process the Personal Data are bound by written confidentiality undertakings or are under an appropriate statutory obligation of confidentiality. Access to Personal Data is granted on a least-privilege, need-to-know basis and logged.

6. Security of processing

The Processor shall implement and maintain the technical and organisational measures set out in **Schedule 2**, having regard to the state of the art, the costs of implementation, the nature, scope, context and purposes of processing, and the risks to data subjects (Art. 32 GDPR).

The measures shall be reviewed at least annually and updated where necessary to reflect new risks or new capabilities.

7. Sub-processors

7.1 General authorisation

The Controller hereby grants the Processor general written authorisation to engage the Sub-processors listed in **Schedule 3** for the processing of Personal Data.

7.2 Obligations on Sub-processors

The Processor shall enter into a written contract with each Sub-processor imposing data protection obligations that are equivalent to those set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures.

7.3 Changes to Sub-processors

The Processor shall give the Controller at least **thirty (30) days' prior written notice** of the addition or replacement of any Sub-processor. The Controller may object on reasonable data protection grounds within that period. If the Parties cannot agree on a resolution, the Controller may terminate the Principal Agreement for convenience, without penalty for unused subscription periods.

7.4 Liability for Sub-processors

The Processor remains fully liable to the Controller for the performance of any Sub-processor's obligations under this DPA.

8. Assistance to the Controller

8.1 Data subject requests

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, in responding to Data Subject Requests. The Processor shall respond to a Controller instruction to action such a request **within seventy-two (72) hours** of receipt.

8.2 Controller obligations under Articles 32-36

The Processor shall assist the Controller in ensuring compliance with its obligations under Articles 32 (security), 33-34 (breach notification), 35 (DPIA) and 36 (prior consultation with a supervisory authority) of the GDPR, taking into account the nature of processing and the information available to the Processor.

9. Security incident notification

9.1 Notification without undue delay

The Processor shall notify the Controller of any Security Incident **without undue delay and in any event within seventy-two (72) hours** of becoming aware of it (Art. 33(2) GDPR).

9.2 Content of the notification

The notification shall at a minimum:

- Describe the nature of the Security Incident, including, where possible, the categories and approximate number of data subjects and records concerned;
- Communicate the name and contact details of the Processor's security contact;
- Describe the likely consequences of the Security Incident;

- Describe the measures taken or proposed to address the Security Incident and mitigate its possible adverse effects.

Where not all information is available within 72 hours, the Processor may provide the information in phases without further undue delay.

9.3 Mitigation and remediation

The Processor shall take all reasonable steps to mitigate the adverse effects of the Security Incident and cooperate with the Controller's investigation and remediation.

10. Return and deletion of Personal Data

Upon termination or expiry of the Principal Agreement, or at any time on the Controller's written instruction, the Processor shall, at the Controller's choice, delete or return all Personal Data to the Controller and delete any existing copies, unless Union or Member State law requires storage of the Personal Data.

Deletion shall be completed within **thirty (30) days** of termination and the Processor shall provide written confirmation of deletion on request.

11. Audit and inspection rights

11.1 Information obligation

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and in Art. 28 GDPR.

11.2 Audits

The Processor shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller, in respect of the processing of Personal Data under this DPA. Such audits shall:

- Be conducted during normal business hours and with reasonable prior notice (at least 30 days, except in the case of an ongoing Security Incident);
- Be conducted no more than once per calendar year, unless a Security Incident, regulator request, or documented material change justifies an additional audit;
- Be subject to reasonable confidentiality undertakings;
- Not unreasonably interfere with the Processor's business activities or compromise the security of other customers.

11.3 Third-party certifications

The Controller agrees that the Processor may satisfy its audit obligations by providing recent third-party audit reports (for example SOC 2, ISO 27001), where available and covering the scope of this DPA.

12. Cross-border transfers

12.1 Default position

Where the Controller is established in the EEA or the United Kingdom, the Processor will, by default, store and process Personal Data in the European Union for customers on the Business tier and above (see Schedule 3).

12.2 Transfers to third countries

Where Personal Data is transferred to a Sub-processor outside the EEA or the UK, the Parties agree that the **Standard Contractual Clauses** adopted by the European Commission by Implementing Decision (EU) 2021/914 ("**SCCs**") are incorporated into this DPA by reference and apply between the Processor (as "data exporter", Module 3: processor-to-processor) and the receiving Sub-processor (as "data importer"). The UK International Data Transfer Addendum ("**UK Addendum**") applies in addition where the Controller is in the United Kingdom.

12.3 Transfer impact

The Processor has carried out a Transfer Impact Assessment for each Sub-processor located outside the EEA / UK. Current TIAs are available on written request.

13. Liability

Liability under this DPA is governed by the liability provisions of the Principal Agreement, save that nothing in the Principal Agreement or this DPA shall limit or exclude either Party's liability for:

- Death or personal injury caused by negligence;
- Fraud or fraudulent misrepresentation;
- Any liability that cannot lawfully be limited or excluded, including claims brought by data subjects under Art. 82 GDPR.

14. Term and termination

This DPA shall remain in force for the duration of the Principal Agreement and, in respect of Personal Data retained after termination, until all Personal Data has been returned or deleted in accordance with section 10.

15. Governing law

This DPA shall be governed by the law of `<<JURISDICTION -- typically England and Wales for UK clients, or the client's home jurisdiction for EU clients>>`, without prejudice to the rights of data subjects under the GDPR.

Schedule 1 -- Details of processing

Item	Details

Nature of processing	Read-only collection of metadata from Controller-authorised workplace tools, combined with voluntary questionnaire responses, to produce an aggregated workflow assessment.
Purpose	Identifying workflow friction and automation opportunities across the Controller's workforce.
Duration of processing	For the term of the Principal Agreement, plus up to 90 days of raw data retention and up to 2 years of aggregated data retention after termination.
Types of Personal Data	Hashed workplace identifiers; activity metadata (counts, timestamps, tool transitions); voluntary free-text questionnaire responses (PII-scrubbed on ingest).
Categories of data subjects	Employees and contractors of the Controller who have workplace tool accounts within the scope agreed between the Parties.
Special categories of data	None intentionally processed. Any incidentally captured special category data is redacted or deleted.
Frequency of transfer	Continuous (API polling, typically hourly or daily depending on source system).
Data importer / exporter	Controller (exporter); Graft Ltd (importer).

Schedule 2 -- Technical and organisational measures

Control area	Measure
Encryption in transit	TLS 1.2 minimum, TLS 1.3 preferred, on all client and inter-service traffic.
Encryption at rest	AES-256-GCM for credential vault (managed by Nango, self-hosted by Graft); database encryption at rest on Neon Postgres.
Credential isolation	Per-organisation OAuth credentials scoped at the Nango connection level; application-layer tenant isolation enforced on every query.

Access control	Role-based access control; least privilege; MFA enforced for all Graft personnel; break-glass procedure for production database access.
Authentication (client-side)	Better Auth with Google SSO, Microsoft Entra SSO, or SCIM-provisioned identities; MFA enforced.
Network security	Vercel CDN + WAF; Neon private endpoints; no public database access.
Logging and monitoring	Pino structured logs; Sentry error monitoring with PII scrubbing; audit log of every query that returns user-level data, retained for 7 years.
Vulnerability management	Dependency scanning on every pull request; quarterly third-party penetration test (planned); responsible-disclosure policy at `security@graft.bot`.
Personnel	Background checks on hire; annual security training; confidentiality undertakings; documented leaver process with same-day credential revocation.
Business continuity	Daily automated database snapshots, 30-day retention; multi-region Vercel deployment; documented recovery time objective of 4 hours and recovery point objective of 24 hours.
Incident response	Documented incident response runbook; 24/7 on-call rotation; 72-hour breach notification.
Data minimisation	Metadata-only ingestion; schema validation rejects unexpected fields; PII detection pass on all free-text fields.
Aggregation threshold	ne5 minimum cohort size enforced in product; differential cell suppression on cross-tabulations.
Secure development	Peer code review required for all changes; CI-enforced lint, type-check, unit, integration and E2E tests; separation of production and non-production environments.
Physical security	All processing is cloud-based on SOC 2 / ISO 27001-certified infrastructure providers. Graft operates no on-premise production hardware.

Schedule 3 -- Sub-processors

The following Sub-processors are authorised as of the date of this DPA.

Sub-processor	Role	Location	Transfer mechanism
Nango (Nango Inc.)	OAuth and integration sync infrastructure. Self-hosted by Graft; vendor does not access customer data.	EU (Frankfurt)	N/A — self-hosted
Neon (Databricks, Inc.)	Serverless Postgres database for application data and metadata	EU (Frankfurt) for Business tier; US for Starter tier	EU SCCs (Module 3) for Starter tier
Vercel (Vercel Inc.)	Hosting, CDN, serverless compute	Global edge; primary compute in EU for Business tier	EU SCCs (Module 3) + UK Addendum
Anthropic (Anthropic, PBC)	Large language model provider (primary) for narrative generation in reports	United States	EU SCCs (Module 3) + UK Addendum + Transfer Impact Assessment
OpenAI (OpenAI, LLC)	Large language model provider (fallback)	United States	EU SCCs (Module 3) + UK Addendum + Transfer Impact Assessment
Sentry (Functional Software, Inc.)	Error monitoring and performance tracing, with PII scrubbing enabled	United States	EU SCCs (Module 3) + UK Addendum + Transfer Impact Assessment

Signatures

Party	Name	Role	Signature	Date
Controller	`<<CLIENT FIELD>>`	`<<CLIENT FIELD>>`		
Processor	`<<GRAFT SIGNATORY>>`	Director, Graft Ltd		

Document control

Field	Value

Version	1.0
Last updated	2026-04-07
Next review	2027-04-07, or on any material change to processing or Sub-processors
Owner	Graft Legal
Source template	Graft GDPR template pack v1.0

Change log

Version	Date	Author	Change
1.0	2026-04-07	Graft	Initial template release