

Customer-facing Data Processing Agreement (DPA)

Finding: Insufficient evidence for Data processing agreement (DPA) — Major

Captured: 2026-09-24T00:34:27.400Z

Org: People Pulse Inc.

This pack provides the **customer-facing** DPA between People Pulse Inc. and its customers (Controller↔Processor), distinct from vendor DPAs with AWS/GitLab.

Data Processing Agreement (Customer-facing)

****Between:**** People Pulse Inc. ("Processor", "PeoplePulse")
****And:**** _____ ("Controller", "Customer")
****Effective date:**** _____ (or date of last signature)
****Related agreement:**** Master Subscription / Order Form between the parties ("Agreement")

This Data Processing Agreement ("DPA") forms part of the Agreement and applies when PeoplePulse processes Personal Data on behalf of Customer in connection with the PeoplePulse services.

1. Roles

- Customer is the Controller (or a Processor instructing PeoplePulse on behalf of a Controller).
- PeoplePulse is the Processor (or Sub-processor) of Personal Data uploaded to or generated in the Services under Customer's instructions.

2. Subject matter & duration

Processing is limited to providing the PeoplePulse SaaS (performance / talent management, surveys, connectors, AI-assisted drafting as enabled by Customer). Duration: term of the Agreement plus any post-termination retention period in §8.

3. Nature & purpose

Host, store, transmit, display, and process Personal Data to deliver the Services; provide support; maintain security/availability; and perform deletions/exports as instructed.

4. Types of Personal Data & data subjects

May include identifiers and employment-related data such as name, work email, job title, manager, org hierarchy, ratings, goals, feedback metadata, and similar HR performance data for Customer's employees/contractors as configured by Customer. Special categories are not intended; Customer shall not submit them unless separately agreed in writing.

5. Instructions

PeoplePulse processes Personal Data only on documented instructions from Customer (including the Agreement, this DPA, and product configuration), unless required by law. PeoplePulse shall inform Customer if an instruction appears to infringe applicable data protection law.

6. Confidentiality & personnel

Personnel authorized to process Personal Data are bound by confidentiality and receive appropriate privacy/security training. Access is role-based and least-privilege.

7. Security

PeoplePulse implements appropriate technical and organizational measures, including: encryption in transit (TLS) and at rest; access control / SSO where configured; audit logging; network segmentation; vulnerability management; and backup of production databases. Details are described in PeoplePulse security documentation provided to Customer.

8. Sub-processors

Customer authorizes PeoplePulse to use sub-processors listed in the then-current sub-processor list (including AWS for hosting). PeoplePulse will impose data-protection terms no less protective than this DPA and remain responsible for sub-processor performance. Material changes will be notified per the Agreement; Customer may object on reasonable data-protection grounds.

9. International transfers

Where Personal Data is transferred internationally, Parties rely on valid transfer mechanisms (e.g., EU SCCs Module 2 Controller→Processor, UK Addendum, or equivalent) attached as Annex C when required.

10. Assistance with data subject rights & DPIA

Taking into account the nature of processing, PeoplePulse assists Customer by appropriate technical/organizational measures for data subject requests and for DPIAs / consultations with supervisory authorities, at Customer's reasonable request.

11. Personal data breach

PeoplePulse will notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data, and will provide information reasonably available to assist Customer's notification obligations.

12. Return / deletion

Upon termination of Services (or earlier written request), PeoplePulse will delete or return Customer Personal Data within thirty (30) days, except copies retained as required by law or in encrypted backups which expire per backup retention schedules. Deletion activity is logged (system, ticket, timestamp, verifier).

13. Audits

Upon reasonable notice, PeoplePulse will make available information necessary to demonstrate compliance with this DPA and will allow audits (or provide third-party audit reports such as SOC 2 when available) no more than once annually, unless required after a breach.

14. Liability & precedence

Liability is as set out in the Agreement. If there is a conflict on data-protection matters, this DPA controls.

Annex A – Processing details

Item	Description
---	---
Systems	PeoplePulse application, managed AWS account/region as contracted
Retention	Per Customer configuration and §12
TOMs summary	Encryption, access control, logging, backups, vulnerability management

Annex B – Sub-processors (illustrative; see live list)

Sub-processor	Purpose	Region
---	---	---
Amazon Web Services	Hosting, database, storage, CDN, email as used	Customer region / US as contracted
Netlify	Marketing site hosting (no customer HR data)	US

Signatures

****Customer (Controller)****

Name: _____ Title: _____ Date: _____ Signature: _____

****People Pulse Inc. (Processor)****

Name: _____ Title: _____ Date: _____ Signature: _____

– End of DPA –