DOCUMENT 02
Data Processing Addendum

WORK DESIGN

Data Processing Addendum

Workplace Priorities App · Schedule 1

How Provider processes Personal Data on the Customer's documented instructions — roles, security, sub-processors, international transfers, and data-subject requests.

SCHEDULE 1 · INCORPORATED INTO THE BUSINESS TERMS OF SERVICE

Data Processing Addendum

Effective date: August 25, 2026 · **Last updated:** August 25, 2026

This Data Processing Addendum (“Addendum”) forms part of the Business Terms of Service between Workspace Design Magazine, LLC (d/b/a Work Design) (“Provider”) and the Customer. It governs Provider’s processing of Personal Data on the Customer’s behalf in connection with the Service.

1. Scope

This Addendum applies to Provider’s processing of Personal Data on Customer’s behalf in connection with the Service.

2. Roles

Customer is the controller, business, or equivalent responsible entity.

Provider is the processor, service provider, contractor, or equivalent processing entity.

Each party is responsible for compliance with obligations applicable to its role.

3. Processing Details

3.1 Subject matter

Providing an AI-assisted workplace survey, analysis, reporting, benchmarking, and related support service.

3.2 Duration

For the duration of the applicable Order Form and the retention period described in the agreement.

3.3 Nature of processing

Collection, receipt, storage, organization, transmission, analysis, aggregation, generation of reports, support, deletion, and other processing necessary to provide the Service.

3.4 Purpose

To administer workplace surveys, analyze responses, generate Customer Reports, provide support, maintain security, and perform Customer’s documented instructions.

3.5 Categories of data subjects

Data subjects may include:

- Customer employees;
- workers and contractors;
- managers and executives;

- survey participants;
- client representatives;
- Authorized Users; and
- other workplace stakeholders invited by Customer.

3.6 Categories of Personal Data

Personal Data may include:

- names and business contact information;
- organizational role or department;
- workplace location;
- survey responses;
- workplace preferences;
- comments and written feedback;
- demographic information expressly configured by Customer;
- unique survey identifiers;
- device and log information; and
- other information submitted by Customer.

3.7 Sensitive Data

Sensitive Data is not intended to be processed except where expressly supported and lawfully configured under Section 12 of the Terms.

4. Documented Instructions

Provider will process Personal Data only:

- on Customer's documented instructions;
- as necessary to provide the Service;
- as described in the agreement; or
- where required by law.

If law requires additional processing, Provider will inform Customer before processing unless legally prohibited.

Provider will notify Customer if it reasonably believes an instruction violates applicable data-protection law.

5. Confidentiality

Provider will ensure that persons authorized to process Personal Data:

- are subject to confidentiality obligations;
- receive appropriate privacy and security instructions; and
- access Personal Data only where necessary.

6. Security

Provider will implement measures appropriate to the risk, taking into account:

- the state of the art;
- implementation costs;
- the nature, scope, context, and purposes of processing; and
- risks to individuals.

Measures may include:

- access controls;
- encryption;
- availability and resilience measures;
- restoration capabilities;
- logging and monitoring;
- vulnerability management;
- incident response;
- backup controls;
- personnel controls; and
- periodic testing.

7. Security Incidents

A “Security Incident” means an accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data processed on Customer’s behalf.

Provider will notify Customer without undue delay after becoming aware of a confirmed Security Incident affecting Customer Personal Data.

The notification will include available information reasonably necessary for Customer to meet applicable notification obligations.

Provider’s notice is not an admission of fault or liability.

8. Subprocessors

Customer grants general authorization for Provider to engage subprocessors.

Provider will:

- maintain a list of material subprocessors;
- impose appropriate data-protection obligations on subprocessors;
- remain responsible for subprocessors’ performance to the extent required by applicable law; and
- provide a mechanism for Customer to receive notice of material new subprocessors.

If Customer reasonably objects to a new subprocessor based on documented data-protection concerns, the parties will attempt to resolve the concern.

If no reasonable resolution is available, Customer may discontinue the affected portion of the Service. Any refund will be determined based on the unused and materially affected portion.

9. Data-Subject Requests

Taking into account the nature of processing, Provider will provide reasonable assistance to Customer with legally valid requests concerning:

- access;
- correction;
- deletion;
- restriction;
- portability;
- objection; and
- rights concerning automated decision-making.

Customer is responsible for verifying requests and communicating with the requester.

10. Compliance Assistance

Taking into account the nature of processing and information available to Provider, Provider will reasonably assist Customer with:

- security obligations;
- Security Incident notifications;
- data-protection impact assessments;
- consultations with supervisory authorities; and
- demonstrating compliance.

Provider may charge reasonable fees for assistance that is unusually burdensome or outside standard Service functionality, except where the need for assistance results from Provider’s breach.

11. Deletion and Return

At the end of the processing services, Provider will delete or return Personal Data at Customer’s choice where reasonably practicable, unless retention is required by law.

Provider may retain information in backups until overwritten under ordinary retention cycles, provided it remains protected and is not used for another purpose.

12. Audits and Information

Provider will make available information reasonably necessary to demonstrate compliance with applicable processor obligations.

Where appropriate, Provider may satisfy audit requests by providing:

- security documentation;
- third-party audit reports;
- certifications;
- questionnaire responses; or
- summaries of relevant controls.

Customer may request an additional audit no more than once annually unless:

- required by a supervisory authority;
- reasonably necessary following a Security Incident; or
- there is credible evidence of material noncompliance.

Audits must:

- A. occur during normal business hours;
- B. avoid unreasonable disruption;
- C. protect other customers' information;
- D. be performed by an independent auditor subject to confidentiality; and
- E. be conducted at Customer's expense unless the audit identifies Provider's material breach.

13. International Transfers

Where required, the applicable European Commission Standard Contractual Clauses are incorporated by reference.

Unless the parties specify otherwise:

- Module Two applies to controller-to-processor transfers;
- the optional docking clause applies;
- the supervisory authority is determined by the exporter's establishment or representative;
- the governing law and courts will be selected as required for valid use of the clauses; and
- the processing details and security measures in this Addendum complete the relevant annexes.

For UK transfers, the applicable UK Addendum or International Data Transfer Agreement is incorporated where required.

The Standard Contractual Clauses or UK transfer mechanism controls over conflicting commercial terms to the extent necessary for validity.

14. U.S. STATE PRIVACY REQUIREMENTS

Provider will:

- process Personal Data only for the business purposes described in the agreement;
- not sell or share Personal Data as legally defined;
- not combine Personal Data received from Customer with unrelated personal information except as legally permitted;
- assist Customer with applicable rights requests;
- notify Customer if Provider can no longer comply with applicable obligations; and
- allow Customer to take reasonable steps to stop and remediate unauthorized processing.

15. Precedence

If this Addendum conflicts with the Terms regarding processing of Personal Data on Customer’s behalf, this Addendum controls.