



MASTER DOCUMENT

Effective August 25, 2026

WORK DESIGN

Terms & Conditions

Workplace Priorities App

The complete, consolidated agreement — Business Terms of Service, Data Processing Addendum, AI Acknowledgment, Participant Notice, and Privacy Notice — in one document.

WORKPLACE PRIORITIES · LEGAL CENTER

Work Design · workdesign.co

Contents

This document consolidates the agreements and notices that govern the Workplace Priorities App. Each part is also available as its own PDF in the Reference Guide.

Business Terms of Service	3
Schedule 1 — Data Processing Addendum	36
Schedule 2 — AI Use Policy & Acknowledgment	42
Schedule 3 — Recommended Participant Notice	44
Privacy Notice	46
Appendix A — Privacy, Data & AI Summary	50

Business Terms of Service

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

These Business Terms of Service, together with any applicable Order Form, Data Processing Addendum, Privacy Notice, service description, and other terms expressly incorporated by reference, constitute a legally binding agreement between:

Workspace Design Magazine, LLC, a Virginia limited liability company (doing business as “Work Design”) with its principal place of business at 904 N Lexington St., Arlington, VA 22205 (“Provider,” “we,” “us,” or “our”), and the individual or legal entity purchasing, accessing, administering, or using the Service (“Customer,” “you,” or “your”).

The individual accepting these Terms on behalf of an organization represents and warrants that the individual has authority to bind that organization.

IMPORTANT AI NOTICE

THE SERVICE USES ARTIFICIAL INTELLIGENCE AND AUTOMATED ANALYTICAL METHODS TO GENERATE SUMMARIES, SCORES, PRIORITIES, OBSERVATIONS, AND RECOMMENDATIONS.

AI-GENERATED OUTPUTS MAY BE INCOMPLETE, INACCURATE, INCONSISTENT, BIASED, MISLEADING, OR UNSUITABLE FOR A PARTICULAR PURPOSE.

THE SERVICE IS A DECISION-SUPPORT AND WORKPLACE-DIAGNOSTIC TOOL. IT IS NOT A SUBSTITUTE FOR PROFESSIONAL JUDGMENT, INDEPENDENT INVESTIGATION, LEGAL ADVICE, HUMAN-RESOURCES ADVICE, EMPLOYMENT-LAW ADVICE, ARCHITECTURAL OR ENGINEERING SERVICES, SAFETY ANALYSIS, ACCESSIBILITY REVIEW, MEDICAL ADVICE, OR OTHER PROFESSIONAL SERVICES.

THE SERVICE MUST NOT BE USED AS THE SOLE OR DETERMINATIVE BASIS FOR ANY DECISION AFFECTING AN IDENTIFIABLE INDIVIDUAL’S EMPLOYMENT, COMPENSATION, PROMOTION, TERMINATION, PERFORMANCE EVALUATION, WORK ASSIGNMENTS, BENEFITS, DISCIPLINE, OR OTHER LEGAL OR ECONOMIC RIGHTS.

BY ACCEPTING THESE TERMS, CUSTOMER EXPRESSLY ACKNOWLEDGES THE AI-BASED NATURE AND LIMITATIONS OF THE SERVICE.

1. Definitions

For purposes of these Terms:

1.1 “Account Data”

“Account Data” means information relating to Customer’s account, authorized users, billing contacts, transaction records, authentication information, and use of the Service.

1.2 “Aggregated Data”

“Aggregated Data” means information derived from multiple customers or participants that has been combined and processed so that it does not identify, and cannot reasonably be used to identify, Customer, an individual participant, or another natural person.

1.3 “AI Components”

“AI Components” means machine-learning models, generative artificial-intelligence models, algorithms, automated classification systems, natural-language-processing systems, statistical systems, prompts, retrieval systems, rules engines, and related technology used in connection with the Service.

1.4 “Authorized User”

“Authorized User” means an employee, contractor, consultant, or professional adviser whom Customer authorizes to access the Service on Customer’s behalf.

1.5 “Customer Content”

“Customer Content” means information, documents, survey questions, participant lists, responses, comments, instructions, configurations, logos, and other content submitted to the Service by or for Customer or its participants.

Customer Content does not include Provider Materials, Usage Data, Aggregated Data, or information that has been properly de-identified.

1.6 “Customer Report”

“Customer Report” means an organization-specific report, scorecard, dashboard, summary, presentation, recommendation, analysis, or other output generated through Customer’s authorized use of the Service.

1.7 “Documentation”

“Documentation” means user instructions, product descriptions, technical materials, support materials, and other documentation that Provider makes available regarding the Service.

1.8 “Order Form”

“Order Form” means an online checkout page, order confirmation, proposal, statement of work, pricing page, or other ordering document identifying the Service purchased by Customer.

1.9 “Participant”

“Participant” means an employee, worker, contractor, manager, stakeholder, or other person invited to complete a survey or provide information through the Service.

1.10 “Personal Data”

“Personal Data” means information defined as personal data, personal information, personally identifiable information, or a similar term under applicable privacy or data-protection law.

1.11 “Provider Materials”

“Provider Materials” means the Service and all related software, source code, object code, technology, workflows, scoring methods, question libraries, taxonomies, prompts, models, algorithms, templates, report formats,

visualizations, methodologies, benchmarks, designs, text, graphics, documentation, know-how, trademarks, and other intellectual property owned, licensed, or developed by Provider.

1.12 “Service”

“Service” means the Workplace Priorities App and associated websites, applications, surveys, AI analysis, reports, dashboards, support, and related services identified in an Order Form.

1.13 “Sensitive Data”

“Sensitive Data” includes special-category data under the GDPR or UK GDPR and any similar legally protected information, including information concerning racial or ethnic origin, religious or philosophical beliefs, political opinions, trade-union membership, genetic information, biometric identifiers, health or disability information, sexual orientation, sex life, precise geolocation, government identification numbers, financial-account credentials, and criminal convictions or allegations.

1.14 “Usage Data”

“Usage Data” means technical and operational information concerning the configuration, performance, security, and use of the Service, excluding identifiable Customer Content except where temporarily necessary to provide security, support, or troubleshooting.

2. Business-To-Business Service

2.1 Business use only

The Service is offered for business and professional use only.

Customer represents that it is acquiring and using the Service primarily for purposes relating to its trade, business, profession, employment responsibilities, or organizational operations, and not primarily for personal, family, or household purposes.

2.2 Minimum age

An individual may not create an account or accept these Terms unless the individual is at least 18 years old and legally capable of entering into a binding agreement.

2.3 Authority

If an individual accesses the Service on behalf of an employer, client, organization, or other legal entity, that individual represents that:

- the individual has authority to act on behalf of that entity;
- the entity has authorized the acquisition and use of the Service;
- the individual has authority to provide the Customer Content submitted through the Service; and
- the entity agrees to be bound by these Terms.

3. The Service

3.1 Workplace diagnostic

The Service is intended to help organizations and workplace professionals collect and evaluate information concerning workplace priorities, employee experiences, preferences, organizational conditions, design considerations, policies, and related topics.

3.2 Service functionality

Depending on the purchased package, the Service may include:

- standardized workplace surveys;
- configurable survey questions;
- survey invitations and response collection;
- aggregated scoring;
- workplace-priority analysis;
- AI-generated summaries and recommendations;
- dashboards, reports, and presentation materials;
- comparison with available benchmarks;
- analysis of open-text responses;
- multi-location or demographic comparisons; and
- other features identified in the applicable Order Form.

3.3 No guaranteed outcome

Provider does not guarantee:

- any minimum response rate;
- that participants will answer accurately or completely;
- that survey respondents represent Customer's overall workforce;
- that any benchmark is statistically representative of Customer's industry or workforce;
- that implementation of a recommendation will produce a particular result;
- that the Service will identify every workplace problem or opportunity; or
- that a Customer Report will satisfy the requirements of any professional, regulatory, contractual, design, employment, or legal process.

3.4 Changes to the Service

Provider may modify, enhance, replace, or discontinue nonmaterial aspects of the Service.

Provider will not materially reduce the core functionality of a purchased one-time assessment after payment unless reasonably necessary to address security, legal compliance, third-party service changes, or circumstances beyond Provider's reasonable control.

4. Orders and Access Rights

4.1 Orders

Customer purchases the right to use the Service as described in the applicable Order Form.

Unless otherwise stated, an Order Form authorizes:

- one Customer organization;
- one survey project;
- one survey population up to the purchased participant limit;
- one primary workplace or organizational assessment;
- one survey launch;
- one reporting cycle; and
- the number of Authorized Users specified in the Order Form.

4.2 Limited license

Subject to Customer's compliance with these Terms and payment of applicable fees, Provider grants Customer a limited, nonexclusive, nontransferable, nonsublicensable, revocable right to access and use the Service during the applicable project period for Customer's internal business purposes and authorized client services.

4.3 Professional client use

A workplace strategist, architect, designer, human-resources consultant, or other professional adviser may use the Service for a client only where:

- the professional has been authorized by the client;
- the professional clearly identifies the organization serving as the data controller or business responsible for participant data;
- the professional provides all required participant notices;
- the professional does not misrepresent the Service as independently validated professional advice;
- the professional complies with confidentiality obligations owed to the client; and
- the professional does not disclose client results without authorization.

4.4 No transfer between clients

Unless an Order Form expressly provides otherwise, an assessment purchased for one client or organization may not be transferred to another client or organization.

5. AI Disclosure and Customer Acknowledgment

5.1 Use of AI

Customer understands that the Service uses AI Components to analyze information and generate outputs.

The particular AI Components used by Provider may change over time.

5.2 Probabilistic operation

AI Components are probabilistic rather than deterministic. Similar inputs may produce different outputs.

Customer acknowledges that outputs may:

- contain factual or logical errors;
- omit relevant information;
- overstate or understate the significance of a finding;
- incorrectly interpret ambiguous responses;
- reflect limitations or biases in submitted information, underlying models, or analytical methods;
- produce recommendations that are not appropriate for Customer's circumstances; or
- appear authoritative despite being incomplete or incorrect.

5.3 Human review required

Customer is solely responsible for reviewing Customer Reports and evaluating them in light of:

- Customer's actual workplace conditions;
- applicable law and regulation;
- professional standards;
- employee and stakeholder input;
- contractual requirements;
- accessibility and safety obligations;
- organizational policies; and
- other relevant information.

Customer must use appropriately qualified human personnel to evaluate material conclusions before relying on them.

5.4 No autonomous decision-making authority

The Service does not have authority to make decisions on behalf of Customer.

Customer will not represent to participants, employees, clients, regulators, or other persons that the Service independently made or approved an organizational or employment decision.

5.5 No professional advice

Outputs are informational and do not constitute:

- legal advice;
- employment or labor-law advice;
- human-resources advice;
- architectural, engineering, or code-compliance advice;
- medical, psychological, or occupational-health advice;
- financial or investment advice;
- cybersecurity advice;
- accessibility certification;

- professional certification; or
- a substitute for services provided by a properly licensed or qualified professional.

5.6 No assurance or certification

Unless expressly stated in an Order Form, the Service does not provide a certification, accreditation, audit opinion, legal conclusion, statistical validation, or assurance that a workplace complies with any standard or law.

5.7 Customer responsibility

Customer remains responsible for all actions, decisions, communications, designs, policies, and recommendations based on or informed by the Service.

6. Restrictions on Employment-Related Use

6.1 Aggregate workplace planning only

The Service is intended for aggregate workplace planning, employee-experience research, organizational strategy, workplace design, programming, policy discussion, change management, and similar decision-support purposes.

6.2 Prohibited individual employment decisions

Customer must not use the Service, Customer Reports, or AI-generated outputs as the sole, primary, determinative, or materially influential basis for:

- recruiting or selecting an individual;
- screening or ranking job applicants;
- hiring, refusing to hire, or terminating an individual;
- promotion, demotion, compensation, or benefits decisions;
- disciplinary action;
- assigning work based on an individual's behavior, traits, personality, or inferred characteristics;
- evaluating individual performance or productivity;
- identifying an individual as a retention, misconduct, or performance risk;
- monitoring individual behavior;
- determining eligibility for employment opportunities; or
- making another decision that produces legal or similarly significant effects for an identifiable person.

6.3 No emotion recognition or biometric categorization

Customer must not use the Service to perform or facilitate:

- emotion recognition;
- biometric identification;
- biometric categorization;
- facial recognition;
- voiceprint analysis;
- personality inference from biometric information; or

- inference of legally protected characteristics.

6.4 No covert employee monitoring

Customer must not use the Service for covert surveillance or monitoring of employees or participants.

6.5 No retaliation

Customer must not retaliate against or disadvantage any Participant for:

- declining to participate;
- withdrawing where withdrawal is legally permitted;
- providing critical feedback;
- exercising privacy rights; or
- raising a concern about the survey or use of results.

6.6 Customer compliance assessment

If Customer intends to use the Service in a manner that could influence individual employment decisions, Customer must not proceed without:

- obtaining Provider's express written approval;
- completing an independent legal and regulatory assessment;
- entering into any additional terms required by Provider;
- implementing documented human oversight;
- providing all legally required notices and explanations; and
- satisfying any applicable high-risk AI, automated-decision-making, employment, labor, discrimination, and data-protection requirements.

Provider may refuse any proposed use that it determines presents an unacceptable legal, ethical, privacy, or reputational risk.

7. Customer Responsibilities

Customer is responsible for:

- determining whether the Service is suitable for Customer's intended use;
- providing accurate account and project information;
- selecting and lawfully inviting Participants;
- determining the lawful basis for collecting and processing Participant information;
- providing legally sufficient notices to Participants;
- obtaining consent where consent is legally required;
- conducting any required consultation with employees, works councils, unions, or worker representatives;
- complying with employment, labor, anti-discrimination, accessibility, privacy, data-protection, and electronic-communications laws;
- ensuring that Customer Content does not violate another person's rights;

- maintaining appropriate internal policies and human oversight;
- protecting the confidentiality of Customer Reports;
- preventing unauthorized access to accounts and reports;
- determining whether a data-protection impact assessment, algorithmic impact assessment, legitimate-interests assessment, or similar review is required;
- responding to Participant questions and complaints; and
- ensuring that Customer's use of the Service is fair, transparent, and consistent with the purposes communicated to Participants.

8. Participant Notice and Survey Administration

8.1 Required notice

Before collecting Participant responses, Customer must provide Participants with a clear notice explaining, as applicable:

- the identity of the organization responsible for the survey;
- the purpose of the survey;
- whether participation is voluntary or required;
- the categories of information collected;
- how responses will be used;
- that AI and automated methods may analyze responses;
- who will receive the results;
- whether responses are anonymous, confidential, pseudonymous, or identifiable;
- applicable response thresholds;
- how long information will be retained;
- whether information will be transferred internationally;
- how Participants may exercise applicable privacy rights; and
- where Participants may obtain additional information.

8.2 Accuracy of confidentiality statements

Customer must not represent that a survey is "anonymous" unless neither Customer nor Provider can reasonably associate responses with identifiable Participants.

If identifiers, unique links, demographic combinations, device information, or other data could permit association with a Participant, Customer must instead use an accurate description such as "confidential," "pseudonymous," or "reported only in aggregate."

8.3 Minimum reporting thresholds

Provider may suppress or combine results where a reporting group contains fewer than five completed responses or where Provider reasonably believes that reporting could enable reidentification.

Customer may not attempt to circumvent reporting thresholds.

8.4 Participant communications

Customer is responsible for the accuracy, legality, and appropriateness of invitations, reminders, survey descriptions, management communications, and representations made to Participants.

9. Accounts and Security

9.1 Account credentials

Customer and Authorized Users must:

- provide accurate registration information;
- keep credentials confidential;
- use individual rather than shared credentials where available;
- use multifactor authentication where offered;
- promptly revoke access for persons who no longer require it; and
- promptly notify Provider of suspected unauthorized access.

9.2 Responsibility for account activity

Customer is responsible for activity occurring through its account, except to the extent caused by Provider's breach of these Terms or failure to maintain reasonable security.

9.3 Administrative control

Customer administrators may be able to:

- invite or remove Authorized Users;
- configure projects;
- access aggregated reports;
- download Customer Reports; and
- manage certain retention and privacy settings.

Customer is responsible for selecting appropriate administrators and limiting their access.

10. Acceptable Use

Customer and Authorized Users must not:

- use the Service unlawfully or fraudulently;
- violate employment, labor, privacy, anti-discrimination, accessibility, or intellectual-property laws;
- upload content they do not have authority to use;
- use the Service to harass, intimidate, discriminate against, or retaliate against another person;
- attempt to identify a Participant from aggregated or de-identified results;
- combine reports with other information for the purpose of reidentifying individuals;
- upload malicious code;
- interfere with the security or operation of the Service;

- probe, scan, or test vulnerabilities without written authorization;
- bypass usage, participant, or account limitations;
- reverse engineer, decompile, disassemble, or attempt to discover source code, models, prompts, scoring logic, or nonpublic methodologies, except where applicable law expressly prohibits such a restriction;
- scrape, copy, or systematically extract Service content;
- use Provider Materials to develop or train a competing product or model;
- resell or sublicense the Service except under an authorized partner or reseller agreement;
- submit false, deceptive, or manipulated survey responses;
- use the Service to generate unlawful, defamatory, or infringing content;
- use the Service for credit, insurance, housing, education admissions, law enforcement, immigration, healthcare eligibility, or other high-impact individual decisions;
- use the Service to infer protected or sensitive characteristics about an individual;
- allow access by a competitor for competitive analysis; or
- use the Service in any manner prohibited by the Documentation.

11. Customer Content

11.1 Customer ownership

As between Customer and Provider, Customer retains all ownership rights it lawfully holds in Customer Content. These Terms do not transfer ownership of Customer Content to Provider.

11.2 Customer license to Provider

Customer grants Provider and its authorized subprocessors a worldwide, nonexclusive, limited license to host, copy, transmit, display, format, analyze, transform, and otherwise process Customer Content solely as reasonably necessary to:

- provide the Service;
- generate Customer Reports;
- provide support;
- maintain security and prevent fraud;
- comply with law;
- enforce these Terms; and
- create Aggregated Data as permitted by Section 14.

This license continues only for as long as necessary for those purposes, subject to applicable retention requirements.

11.3 Customer warranties

Customer represents and warrants that:

- Customer has all rights and authority necessary to provide Customer Content;
- Customer's instructions comply with applicable law;

- processing Customer Content as contemplated by these Terms will not violate another person's rights;
- Customer has provided all required notices;
- Customer has obtained all required permissions and consents; and
- Customer Content does not contain prohibited information.

11.4 Customer responsibility for content

Provider is not responsible for verifying the accuracy, completeness, legality, or representativeness of Customer Content.

Provider may remove, quarantine, or restrict Customer Content that it reasonably believes violates these Terms or applicable law.

12. Sensitive and Prohibited Data

12.1 Data minimization

Customer will submit only information reasonably necessary for the stated workplace-assessment purpose.

12.2 Prohibited information

Customer must not submit:

- Social Security numbers or national identification numbers;
- passport or driver's-license numbers;
- bank-account or payment-card information;
- account passwords or authentication secrets;
- medical records or detailed clinical information;
- biometric templates;
- precise real-time geolocation;
- information concerning children under 18;
- classified government information;
- export-controlled technical data;
- attorney-client privileged material unless expressly agreed in writing; or
- another category of information that Provider identifies as unsupported.

12.3 Sensitive demographic information

Customer may collect Sensitive Data through the Service only where:

- the relevant feature is expressly supported;
- collection is necessary and proportionate;
- Customer has established a valid legal basis;
- explicit consent has been obtained where required;
- participation is genuinely voluntary where required;
- Customer has completed any legally required impact assessment;

- the information is used only for lawful aggregate analysis;
- reporting thresholds are applied; and
- the information is not used to make decisions concerning identifiable individuals.

12.4 Provider's right to disable fields

Provider may disable, suppress, or delete fields or responses that create an unreasonable privacy, discrimination, or reidentification risk.

13. Data-Protection Roles

13.1 Customer as controller

For Personal Data contained in Participant lists, survey responses, demographic information, comments, and related Customer Content, Customer generally acts as the:

- “controller” under the GDPR and UK GDPR;
- “business” under the California Consumer Privacy Act, where applicable; or
- equivalent responsible party under applicable privacy law.

13.2 Provider as processor

To the extent Provider processes such Personal Data solely on Customer's documented instructions to provide the Service, Provider acts as Customer's:

- “processor” under the GDPR and UK GDPR;
- “service provider” or “contractor” under the California Consumer Privacy Act, where applicable; or
- equivalent service provider under applicable law.

13.3 Provider as independent controller

Provider may act as an independent controller or business for Account Data and information processed for:

- account administration;
- billing and payment records;
- fraud prevention;
- Service security;
- legal compliance;
- direct communications with Customer representatives;
- product analytics involving Provider's own business operations; and
- establishing, exercising, or defending legal claims.

13.4 Data Processing Addendum

The Data Processing Addendum in Schedule 1 applies where Provider processes Personal Data on Customer's behalf.

If a separately executed Data Processing Addendum conflicts with Schedule 1, the separately executed addendum controls with respect to that conflict.

14. Aggregated and De-Identified Data

14.1 Right to create Aggregated Data

Provider may create Aggregated Data from Customer Content and Usage Data, provided that Provider uses reasonable measures designed to prevent the data from identifying Customer or an individual.

14.2 Permitted uses

Provider may use Aggregated Data to:

- operate and improve the Service;
- evaluate performance and accuracy;
- develop benchmarks;
- conduct statistical and workplace research;
- identify product trends;
- develop new features;
- publish industry-level insights;
- improve security; and
- support marketing claims based on aggregate statistics.

14.3 No customer identification

Provider will not publicly identify Customer as the source of Aggregated Data without Customer's permission.

14.4 No reidentification

Provider will not attempt to reidentify properly de-identified Participant information except where reasonably necessary to test whether de-identification controls are effective or where required by law.

14.5 Ownership

As between the parties, Provider owns Aggregated Data and generalized statistical findings that do not identify Customer or a Participant.

Customer retains ownership of the underlying Customer Content.

15. AI Model Training and Product Improvement

15.1 No general-purpose training using identifiable content

Provider will not use identifiable Customer Content or identifiable Participant responses to train a general-purpose AI model for use across unrelated customers unless Customer has given separate, express, written or electronic opt-in consent.

Acceptance of these Terms alone does not constitute such opt-in consent.

15.2 Service-specific improvement

Provider may use:

- Aggregated Data;
- properly de-identified data;
- synthetic data;
- Customer feedback;
- technical telemetry; and
- manually reviewed examples that have been stripped of Customer and Participant identifiers,

to evaluate and improve the Service.

15.3 Third-party AI providers

Provider will configure third-party AI providers, where commercially available and appropriate, so that Customer Content is not used by those providers to train general-purpose models.

Provider's current subprocessor list will identify material third-party AI and hosting providers.

15.4 Customer-selected integrations

If Customer directs Provider to transmit Customer Content to a third-party service selected or controlled by Customer, that third party's terms and privacy practices apply to the third party's processing.

16. Customer Reports and Output Rights

16.1 Customer's use of Customer Reports

Subject to payment of applicable fees, Provider grants Customer a perpetual, worldwide, nonexclusive right to use, reproduce, distribute, display, adapt, and incorporate Customer Reports into Customer's internal business activities and authorized professional services.

16.2 Client reports

A professional adviser may provide a Customer Report to the client for whom the report was generated.

The professional may not:

- use one client's report for another client;
- disclose confidential client information;
- remove legally required AI disclosures;
- misrepresent AI-generated findings as independently verified conclusions; or
- sell the report as a certification issued by Provider unless expressly authorized.

16.3 Underlying Provider Materials

Customer's rights in a Customer Report do not transfer ownership of:

- the Service;
- scoring methodologies;

- standard survey questions;
- benchmark databases;
- report templates;
- prompts;
- AI Components;
- taxonomies;
- analytical frameworks; or
- other Provider Materials embedded in or used to create the report.

16.4 Similar outputs

Because AI systems and standardized methodologies may generate similar content for different customers, Customer does not receive exclusive rights to general ideas, generalized recommendations, structures, phrasing, or outputs that do not contain Customer's confidential information.

16.5 Legal availability of rights

AI-generated material may not qualify for intellectual-property protection in every jurisdiction. Provider does not warrant that Customer Reports are copyrightable, patentable, registrable, unique, or free from similarity to other materials.

17. Provider Intellectual Property

17.1 Provider ownership

Provider and its licensors retain all rights, title, and interest in Provider Materials.

No rights are granted except those expressly stated in these Terms.

17.2 Restrictions

Customer may not:

- copy or distribute Provider Materials except as permitted;
- remove proprietary notices;
- create a competing survey, benchmark, model, or service using Provider Materials;
- publish the Service's nonpublic scoring system;
- use report templates independently of the Service to provide a competing automated product; or
- claim ownership of Provider's methodology.

17.3 Feedback

If Customer provides suggestions, recommendations, enhancement requests, corrections, or other feedback, Customer grants Provider a perpetual, irrevocable, worldwide, royalty-free right to use that feedback without restriction or payment.

Provider will not identify Customer as the source of public feedback without permission.

18. Confidentiality

18.1 Confidential Information

“Confidential Information” means nonpublic information disclosed by one party to the other that:

- is identified as confidential;
- should reasonably be understood to be confidential; or
- concerns business operations, clients, technology, security, pricing, survey responses, Customer Reports, methods, or product plans.

Customer Content and nonpublic Customer Reports are Customer’s Confidential Information.

Nonpublic Provider Materials are Provider’s Confidential Information.

18.2 Use and protection

The receiving party will:

- use Confidential Information only to perform or exercise rights under the agreement;
- protect it using at least reasonable care;
- disclose it only to personnel, advisers, and contractors who need to know it and are bound by appropriate confidentiality obligations; and
- not disclose it to another person except as authorized.

18.3 Exclusions

Confidential Information does not include information that the receiving party can demonstrate:

- was lawfully known without restriction before disclosure;
- becomes public without breach of the agreement;
- is received lawfully from a third party without confidentiality restriction; or
- is independently developed without use of the disclosing party’s Confidential Information.

18.4 Legally compelled disclosure

The receiving party may disclose Confidential Information where legally required, provided that, unless prohibited by law, it gives reasonable notice and assistance to the disclosing party.

18.5 Equitable relief

Unauthorized use or disclosure of Confidential Information may cause harm that cannot be fully remedied by damages. The disclosing party may seek appropriate injunctive or equitable relief in addition to other remedies.

19. Privacy

19.1 Privacy Notice

Provider’s Privacy Notice explains how Provider processes Personal Data in its role as an independent controller or business.

19.2 Customer privacy obligations

Customer is responsible for its own privacy notices, lawful bases, consent mechanisms, employee communications, and responses to Participant rights requests.

19.3 Rights requests

If Provider receives a request from a Participant concerning Personal Data processed solely on Customer's behalf, Provider may refer the request to Customer.

Provider will provide reasonable assistance as described in the Data Processing Addendum.

19.4 No sale of Participant data

Provider will not sell Participant Personal Data or share it for cross-context behavioral advertising as those terms are defined under applicable U.S. state privacy laws.

19.5 Marketing

Provider will not use Participant contact information submitted solely for survey administration to market unrelated products directly to Participants.

20. Information Security

20.1 Security program

Provider will maintain reasonable administrative, technical, and organizational safeguards designed to protect Personal Data against unauthorized access, acquisition, alteration, disclosure, loss, or destruction.

20.2 Security measures

Depending on the nature and maturity of the Service, safeguards may include:

- encryption in transit;
- encryption at rest where appropriate;
- access controls;
- authentication controls;
- logging and monitoring;
- vulnerability management;
- incident-response procedures;
- backups and recovery controls;
- personnel confidentiality requirements;
- vendor-risk management; and
- periodic security reviews.

20.3 No absolute security guarantee

No information system is completely secure. Provider does not guarantee that unauthorized access, security incidents, or data loss can never occur.

20.4 Customer security

Customer is responsible for:

- securing its own devices and networks;
- protecting downloaded reports;
- controlling Authorized User access;
- using secure email and file-sharing practices; and
- notifying Provider promptly of suspected compromise.

21. Subprocessors and International Transfers

21.1 Subprocessors

Customer authorizes Provider to use subprocessors to provide hosting, analytics, communications, payment processing, customer support, AI functionality, and related services.

21.2 Subprocessor list

Provider will maintain a current list of material subprocessors at workdesign.co/legal/subprocessors.

21.3 Subprocessor obligations

Provider will enter into written agreements requiring subprocessors that process Personal Data on Provider's behalf to protect that data consistently with applicable law and the Data Processing Addendum.

21.4 International transfers

Where Personal Data is transferred from the European Economic Area, United Kingdom, or Switzerland to a country not recognized as providing adequate protection, the parties will use an appropriate transfer mechanism, which may include:

- the European Commission's Standard Contractual Clauses;
- the UK International Data Transfer Addendum;
- the UK International Data Transfer Agreement;
- another approved transfer mechanism; or
- an applicable adequacy decision.

21.5 Transfer assessments

The parties will reasonably cooperate in completing legally required transfer-risk assessments and implementing supplementary safeguards.

22. Retention and Deletion

22.1 Project retention period

Unless otherwise stated in an Order Form or account setting, Provider may retain identifiable Customer Content for 365 days after completion of the project.

22.2 Customer-selected deletion

Customer may request deletion of Customer Content, subject to:

- legal-retention obligations;
- fraud and security requirements;
- backup cycles;
- dispute preservation; and
- technical limitations described in the Data Processing Addendum.

22.3 Reports

Customer is responsible for downloading any Customer Reports it wishes to retain before account or project deletion.

22.4 Backups

Deleted information may remain in encrypted or access-restricted backups until overwritten in the ordinary course of Provider's backup-retention process.

22.5 Aggregated Data

Deletion of Customer Content does not require deletion of Aggregated Data that no longer identifies Customer or a Participant.

23. Third-Party Services

23.1 Third-party dependencies

The Service may depend on third-party hosting providers, AI providers, payment processors, email providers, analytics providers, or other services.

23.2 Third-party outages

Provider is not responsible for failures caused by third-party services beyond Provider's reasonable control, but Provider will use commercially reasonable efforts to restore affected functionality.

23.3 Third-party links

The Service may include links to third-party websites. Provider does not control and is not responsible for those websites.

23.4 Payment processor

Payment-card information may be processed directly by Stripe, Inc. Provider may not receive or store complete payment-card numbers.

The payment processor's terms and privacy notice apply to its processing.

24. Fees and Payment

24.1 Fees

Customer will pay the fees stated in the applicable Order Form.

24.2 One-time purchase

Unless the Order Form expressly states otherwise, each purchase is a one-time purchase for the specified assessment and does not automatically renew.

24.3 Participant limits

Fees may be based on the number of Participants invited, rather than the number who complete the survey.

Customer may not exceed the purchased participant limit without paying applicable additional fees.

24.4 Taxes

Fees exclude applicable sales, use, value-added, goods-and-services, withholding, or similar taxes unless the Order Form states otherwise.

Customer is responsible for applicable taxes other than taxes based on Provider's net income.

24.5 Payment authorization

Customer authorizes Provider and its payment processor to charge the payment method provided for all amounts due.

24.6 Failed payments

Provider may suspend activation or access where payment is declined, reversed, disputed, or overdue.

24.7 Currency

Fees will be charged in the currency identified at checkout or on the Order Form.

Customer is responsible for foreign-exchange charges and bank fees.

24.8 Promotional pricing

Discounts, referral codes, partner pricing, and promotional offers:

- apply only under the stated conditions;
- may not be combined unless expressly permitted;
- have no cash value;
- may be revoked in cases of misuse; and
- do not change the list price of future purchases.

25. Cancellations and Refunds

25.1 Pre-activation cancellation

Unless otherwise stated, Customer may request cancellation within seven days after purchase if:

- no Participant invitations have been sent;

- no Customer Content has been submitted for AI analysis;
- no Customer Report has been generated; and
- Provider has not begun material custom work.

Provider may deduct nonrecoverable payment-processing fees where permitted by law.

25.2 Activated projects

Once Participant invitations have been sent, AI processing has begun, or a Customer Report has been generated, fees are nonrefundable except where:

- Provider fails to provide the purchased Service;
- applicable law requires a refund; or
- Provider agrees otherwise in writing.

25.3 Customer delays

Customer is not entitled to a refund because:

- Participants fail to respond;
- Customer does not launch the survey;
- Customer does not download the report;
- Customer changes its project plans; or
- Customer does not use all purchased participant capacity.

25.4 Expiration

Unless otherwise stated, an unused one-time assessment must be activated within 12 months after purchase.

25.5 Mandatory rights

Nothing in this Section limits nonwaivable statutory rights that apply despite the business-use requirements in these Terms.

26. Support

26.1 Standard support

Provider will provide the support described in the applicable Order Form or Documentation.

26.2 Support limitations

Standard support does not include:

- legal advice;
- survey-methodology consulting;
- workplace-strategy consulting;
- custom statistical analysis;
- architectural or design advice;
- custom data migration;

- employee relations support; or
- support for third-party systems.

26.3 Professional services

Additional implementation, interpretation, workshop, consulting, or customization services may be subject to separate fees and terms.

27. Service Availability

27.1 Availability

Provider will use commercially reasonable efforts to make the Service available but does not guarantee uninterrupted or error-free operation.

27.2 Maintenance

Provider may conduct maintenance that temporarily affects availability.

Where reasonably practicable, Provider will provide advance notice of planned material maintenance.

27.3 Force majeure

Provider is not responsible for delay or failure caused by circumstances beyond its reasonable control, including natural disasters, utility failures, internet failures, labor disputes, war, terrorism, civil unrest, governmental action, epidemics, cyberattacks, or failures of third-party infrastructure.

28. Beta and Experimental Features

Provider may identify certain features as beta, preview, pilot, experimental, or evaluation features.

Such features:

- may be incomplete;
- may change or be withdrawn;
- may produce less reliable results;
- may not be covered by all support commitments; and
- should not be used for material decisions without additional review.

To the maximum extent permitted by law, beta features are provided “as is.”

29. Warranties

29.1 Authority warranty

Each party warrants that it has authority to enter into the agreement.

29.2 Provider performance warranty

Provider warrants that it will provide the Service in a professional and commercially reasonable manner consistent with the applicable Documentation.

29.3 Exclusive remedy

If Customer reports a material breach of the warranty in Section 29.2 within 30 days after delivery, Provider will use commercially reasonable efforts to correct the nonconformity.

If Provider cannot correct it within a reasonable period, Customer may terminate the affected Order Form and receive a prorated or reasonable refund for the materially deficient portion of the Service.

This is Customer's exclusive contractual remedy for breach of Section 29.2.

30. Disclaimers

TO THE MAXIMUM EXTENT PERMITTED BY LAW, EXCEPT FOR THE EXPRESS WARRANTY IN SECTION 29:

THE SERVICE, AI COMPONENTS, CUSTOMER REPORTS, BENCHMARKS, AND RECOMMENDATIONS ARE PROVIDED "AS IS" AND "AS AVAILABLE";

PROVIDER DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, ACCURACY, QUIET ENJOYMENT, AND WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE;

PROVIDER DOES NOT WARRANT THAT OUTPUTS WILL BE ACCURATE, COMPLETE, UNIQUE, UNBIASED, ERROR-FREE, OR SUITABLE FOR CUSTOMER'S PURPOSES;

PROVIDER DOES NOT WARRANT THAT THE SERVICE WILL COMPLY WITH LAWS OR PROFESSIONAL STANDARDS APPLICABLE TO CUSTOMER'S PARTICULAR USE;

PROVIDER DOES NOT WARRANT THAT CUSTOMER CONTENT OR OUTPUTS WILL BE PRESERVED INDEFINITELY;

PROVIDER DOES NOT WARRANT THAT USE OF THE SERVICE WILL IMPROVE EMPLOYEE SATISFACTION, PRODUCTIVITY, RETENTION, ATTENDANCE, SPACE UTILIZATION, CULTURE, OR FINANCIAL PERFORMANCE; AND

PROVIDER IS NOT RESPONSIBLE FOR DECISIONS MADE BY CUSTOMER, ITS CLIENTS, OR THEIR PERSONNEL.

Some jurisdictions do not allow certain disclaimers. In those jurisdictions, the disclaimers apply only to the maximum extent permitted by law.

31. Customer Indemnification

Customer will defend, indemnify, and hold harmless Provider, its affiliates, and their officers, directors, employees, contractors, and agents from third-party claims, damages, judgments, penalties, costs, and reasonable legal fees arising from:

- Customer Content;
- Customer's unlawful collection or use of Participant data;
- Customer's failure to provide required notices or obtain required permissions;
- Customer's employment, workforce, design, policy, or other decisions;
- Customer's use of the Service in violation of Sections 6, 7, 8, 10, or 12;
- Customer's infringement or violation of another person's rights;
- Customer's misrepresentation of Customer Reports or the Service; or
- Customer's breach of applicable employment, labor, discrimination, privacy, or data-protection law.

Provider will:

- promptly notify Customer of an indemnified claim;
- permit Customer to control the defense and settlement; and
- provide reasonable cooperation at Customer's expense.

Customer may not settle a claim in a manner that admits wrongdoing by Provider, imposes an obligation on Provider, or restricts Provider's operations without Provider's written consent.

32. Provider Intellectual-Property Indemnification

32.1 Covered claims

Provider will defend Customer against a third-party claim that Customer's authorized use of the Service directly infringes that third party's registered copyright, patent, or trademark, and will pay damages finally awarded or agreed in settlement.

32.2 Exclusions

Provider has no obligation for claims arising from:

- Customer Content;
- Customer's modification of the Service or Customer Report;
- use in combination with items not supplied by Provider;
- use outside the Documentation;
- continued use after Provider has notified Customer to stop;
- compliance with Customer's instructions;
- open-source or third-party components governed by separate terms; or
- AI-generated similarities that do not result from Provider's intentional copying.

32.3 Remedies

If the Service is likely to become subject to an infringement claim, Provider may:

- obtain the right for Customer to continue using it;
- modify or replace the affected functionality; or
- terminate the affected Order Form and refund a reasonable portion of the fees.

This Section states Provider's entire obligation regarding third-party intellectual-property infringement claims.

33. Limitation of Liability

33.1 Excluded damages

TO THE MAXIMUM EXTENT PERMITTED BY LAW, NEITHER PARTY WILL BE LIABLE FOR:

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES;

LOST PROFITS, REVENUE, SAVINGS, GOODWILL, OR BUSINESS OPPORTUNITIES;

LOSS OR CORRUPTION OF DATA;

BUSINESS INTERRUPTION;

COSTS OF SUBSTITUTE SERVICES; OR

DAMAGES ARISING FROM EMPLOYMENT, DESIGN, REAL-ESTATE, CONSTRUCTION, POLICY, OR MANAGEMENT DECISIONS,

EVEN IF THE PARTY WAS ADVISED THAT SUCH DAMAGES WERE POSSIBLE.

33.2 General liability cap

Except as stated in Sections 33.3 and 33.4, each party's total aggregate liability arising from or relating to the agreement will not exceed the greater of:

- the fees paid or payable by Customer under the Order Form giving rise to the claim; or
- US \$1,000.

33.3 Enhanced liability cap

Provider's total aggregate liability arising from:

- Provider's breach of confidentiality obligations;
- a Security Incident caused by Provider's material failure to comply with its contractual security obligations; or
- Provider's obligations under Section 32,

will not exceed the greater of:

- two times the fees paid or payable under the affected Order Form; or
- US \$10,000.

A negotiated enterprise Order Form may specify a different enhanced cap.

33.4 Exclusions from caps

Nothing in the agreement limits liability to the extent it cannot lawfully be limited, including liability for:

- fraud or fraudulent misrepresentation;
- willful misconduct;
- death or personal injury caused by negligence where such liability cannot be limited;
- Customer's payment obligations;
- Customer's unauthorized use or infringement of Provider Materials; or
- another category that applicable law prohibits the parties from limiting.

33.5 Allocation of risk

The parties agree that the fees reflect the allocation of risk in these Terms and that the limitations are an essential basis of the bargain.

34. Suspension

Provider may suspend access where reasonably necessary to:

- prevent or address a security threat;
- prevent unlawful or prohibited use;
- protect Participants or third parties;
- respond to a legal or regulatory requirement;
- address nonpayment;
- investigate suspected fraud;
- prevent material harm to the Service; or
- address a material breach of these Terms.

Where reasonably practicable, Provider will notify Customer and provide an opportunity to cure.

35. Termination

35.1 Termination for breach

Either party may terminate an Order Form or the agreement if the other party materially breaches it and fails to cure the breach within 30 days after written notice.

A cure period is not required where the breach:

- is incapable of cure;

- involves unlawful conduct;
- creates a material security or privacy risk;
- involves misuse of intellectual property; or
- justifies immediate termination under applicable law.

35.2 Provider termination

Provider may terminate the agreement or discontinue the Service upon reasonable notice where Provider ceases operating the applicable product.

If Provider terminates an activated, paid project for convenience before delivering the purchased Service, Provider will provide a reasonable refund for the undelivered portion.

35.3 Effect of termination

Upon termination:

- Customer's right to access the Service ends;
- fees already accrued remain due;
- Customer should download available Customer Reports before the termination date;
- Provider may delete Customer Content in accordance with its retention schedule; and
- provisions that by their nature should survive will survive.

35.4 Surviving provisions

Sections concerning ownership, confidentiality, payment, disclaimers, indemnification, liability, disputes, and general contractual provisions survive termination.

36. Publicity

Provider may not use Customer's name, logo, trademarks, survey results, or case-study information in publicity without Customer's prior permission.

Customer may identify itself as a user of the Service, provided it does not imply endorsement, certification, or partnership beyond the parties' actual relationship.

37. Compliance with Law

Each party will comply with laws applicable to its own performance under the agreement.

Customer is specifically responsible for laws applicable to:

- Customer's workforce;
- Participant communications;
- workplace monitoring;
- employment decisions;
- labor consultation;
- accessibility;

- retention of personnel information;
- professional licensing;
- surveys and research; and
- use of AI-generated recommendations.

38. Export Controls and Sanctions

Customer will not access, use, export, or re-export the Service in violation of applicable export-control, trade-sanctions, or anti-boycott laws.

Customer represents that it and its Authorized Users are not prohibited or restricted parties under applicable sanctions laws.

39. Anti-Bribery

Neither party will offer, promise, authorize, solicit, or accept an improper payment, benefit, or inducement in connection with the agreement.

Referral fees, partner commissions, and discounts must be disclosed where required and must comply with Customer's professional, ethical, procurement, and employer policies.

40. Dispute Resolution

40.1 Good-faith resolution

Before filing a formal claim, the complaining party will provide written notice describing the dispute.

The parties will attempt in good faith to resolve the dispute through discussions between authorized representatives for at least 30 days.

40.2 Governing law

Except to the extent mandatory law requires otherwise, the agreement is governed by the laws of the Commonwealth of Virginia, United States, without regard to conflict-of-laws principles.

40.3 Courts

Subject to Section 40.1, the parties consent to the exclusive jurisdiction of:

- the state courts located in Arlington County, Virginia; and
- the United States District Court for the Eastern District of Virginia.

Each party waives objections based on venue or inconvenient forum.

40.4 Injunctive relief

Either party may seek immediate injunctive or equitable relief for actual or threatened misuse of intellectual property, Confidential Information, Personal Data, or system security.

40.5 No class or representative actions

To the extent permitted by law, each party will bring claims only in its individual or organizational capacity and not as a plaintiff or member of a class, collective, consolidated, or representative proceeding.

40.6 Mandatory local law

Nothing in this Section deprives a party of rights or remedies that cannot legally be waived by agreement.

41. Changes to These Terms

41.1 Prospective changes

Provider may update these Terms to reflect:

- changes to the Service;
- changes in law;
- security or privacy developments;
- changes in business practices; or
- new features.

41.2 Notice

Provider will provide reasonable notice of material changes by email, in-product notice, account notification, or another reasonable method.

41.3 Existing purchased projects

Material changes will not retroactively reduce Customer's rights or materially expand Provider's right to use identifiable Customer Content for an already purchased project without Customer's affirmative agreement, unless the change is required by law.

41.4 Continued use

Continued use after the effective date of updated Terms constitutes acceptance where permitted by law.

If Customer does not agree, Customer must stop using the Service.

42. Notices

Legal notices to Provider must be sent to:

Workspace Design Magazine, LLC (d/b/a Work Design)

904 N Lexington St.

Arlington, VA 22205

Email: bob.fox@workdesign.com

Provider may send notices to the account administrator or billing contact identified by Customer.

Email notices are deemed received on the next business day after sending unless the sender receives a delivery-failure notification.

43. General Provisions

43.1 Entire agreement

The agreement constitutes the entire agreement concerning the Service and supersedes prior or contemporaneous discussions, representations, and agreements concerning its subject matter.

43.2 Order of precedence

In the event of conflict, the following order applies:

- a signed negotiated Order Form;
- a signed Data Processing Addendum;
- the schedules to these Terms;
- these Terms;
- the Privacy Notice; and
- the Documentation.

A Privacy Notice does not override contractual data-processing restrictions.

43.3 Assignment

Customer may not assign the agreement without Provider's prior written consent, except in connection with a merger, reorganization, or sale of substantially all relevant assets, provided the assignee is not a direct competitor and agrees to be bound.

Provider may assign the agreement in connection with a merger, reorganization, financing, or sale of its business or assets.

43.4 Independent contractors

The parties are independent contractors.

The agreement does not create an employment, agency, fiduciary, partnership, franchise, or joint-venture relationship.

43.5 No third-party beneficiaries

Except for indemnified parties expressly identified in these Terms, the agreement creates no third-party beneficiary rights.

43.6 Waiver

Failure to enforce a provision is not a waiver.

A waiver must be in writing and applies only to the specific circumstance identified.

43.7 Severability

If a provision is held invalid or unenforceable, it will be modified to the minimum extent necessary to make it enforceable, and the remaining provisions will remain effective.

43.8 Interpretation

Headings are for convenience only.

“Including” means “including without limitation.”

The singular includes the plural and vice versa where appropriate.

43.9 Electronic agreement

Electronic acceptance, including checking a box, clicking an acceptance button, creating an account, or using the Service after being presented with these Terms, has the same effect as a handwritten signature.

43.10 Language

The English-language version controls to the extent permitted by law.

Any translation is provided for convenience unless the parties expressly agree otherwise.

44. Regional Terms

44.1 European Economic Area

Where the GDPR applies:

- the parties will comply with the Data Processing Addendum;
- Customer is responsible for determining a lawful basis for processing;
- Customer is responsible for providing information required by Articles 13 and 14 of the GDPR;
- Customer will not instruct Provider to conduct prohibited or unlawful automated decision-making;
- Customer will complete a data-protection impact assessment where required;
- international transfers will be handled under Section 21 and Schedule 1;
- Customer will implement appropriate human review where processing involves profiling or decisions concerning individuals; and
- nothing in the agreement limits rights or obligations that cannot be contractually waived under the GDPR.

44.2 United Kingdom

Where the UK GDPR or Data Protection Act 2018 applies:

- references to the GDPR will be interpreted to include the UK GDPR where appropriate;
- international-transfer mechanisms may include the UK International Data Transfer Agreement or UK Addendum;
- Customer is responsible for worker notices and any required consultation; and
- the parties will comply with applicable Information Commissioner guidance and binding legal requirements.

44.3 California and other U.S. states

Where Provider processes Personal Data as a service provider, contractor, or processor under applicable U.S. state privacy law:

- Provider will process the data only for the limited and specified purposes described in the agreement;
- Provider will not sell the data;
- Provider will not share the data for cross-context behavioral advertising;

- Provider will not retain, use, or disclose the data outside the direct business relationship except as legally permitted;
- Provider will provide the same level of privacy protection required by applicable law;
- Provider will notify Customer if it determines that it can no longer meet its applicable obligations;
- Customer may take reasonable and appropriate steps to help ensure compliant processing; and
- Provider will cooperate with Customer regarding legally valid consumer requests.

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.

AI Use Policy & Acknowledgment

Workplace Priorities uses artificial intelligence and automated analytical methods to generate summaries, scores, priorities, observations, and recommendations. Our approach to AI is governed by the Business Terms of Service (notably Sections 5 and 6) and summarized here.

AI IS DECISION-SUPPORT, NOT A DECISION-MAKER

AI outputs can be incomplete or inaccurate and must be reviewed by appropriately qualified people before any material decision. The Service has no authority to make decisions on anyone's behalf and is not a substitute for professional, legal, HR, design, or engineering judgment.

NEVER FOR INDIVIDUAL EMPLOYMENT DECISIONS

Results must never be the sole or determinative basis for hiring, termination, promotion, compensation, discipline, or individual performance evaluation. The Service does not perform emotion recognition, biometric categorization, covert monitoring, or inference of protected characteristics.

YOUR CONTENT IS NOT USED TO TRAIN GENERAL AI MODELS

Identifiable customer content and participant responses are not used to train general-purpose AI models for other customers without separate, express opt-in consent, and third-party AI providers are configured so that customer content is not used to train their general models.

SCHEDULE 2 · REQUIRED AI AND WORKPLACE-USE ACKNOWLEDGMENT

Before launching a survey, the Customer must affirmatively acknowledge each of the following:

- I understand that the Service uses artificial intelligence and automated analysis.
- I understand that AI-generated outputs may be inaccurate, incomplete, biased, inconsistent, or unsuitable.
- I will ensure that qualified people review material findings before they are used.
- I will not use the Service as the sole or determinative basis for decisions affecting an identifiable person.
- I will not use the Service to recruit, screen, rank, hire, fire, promote, discipline, compensate, monitor, or evaluate an identifiable individual.
- I am responsible for providing legally required notices to survey participants.
- I am responsible for determining the lawful basis for collecting and using participant information.
- I will not represent a survey as anonymous unless it is genuinely anonymous.
- I will not attempt to identify participants from aggregated results.
- I will not retaliate against anyone because of participation, nonparticipation, survey responses, or exercise of privacy rights.
- I will use Customer Reports as decision-support materials and not as legal, architectural, engineering, human-resources, medical, or other professional advice.
- I have authority to act for the Customer organization and to submit the information provided.

Checkbox text. ☐ I have read and agree to the Business Terms of Service, Data Processing Addendum, Privacy Notice, and AI and Workplace-Use Acknowledgment.

Recommended Participant Notice

This is a **fill-in template**. Replace every highlighted field, and select exactly one confidentiality statement, before sending it to participants. It does not replace your organization's own employee privacy notice.

ABOUT THIS WORKPLACE SURVEY

[ORGANIZATION NAME]

... is conducting this survey to better understand workplace experiences, priorities, and opportunities. The survey is administered using the Workplace Priorities App, an AI-assisted survey and analysis platform provided by Work Design (Workspace Design Magazine, LLC).

Artificial intelligence and automated analytical methods may be used to organize responses, identify themes, calculate scores, summarize comments, and generate recommendations. AI-generated findings may be incomplete or inaccurate and will be reviewed by appropriate personnel before material decisions are made.

HOW YOUR INFORMATION WILL BE USED

Your responses will be used for workplace planning, organizational strategy, employee-experience evaluation, workplace design, policy discussion, or related purposes described here:

[INSERT SPECIFIC PURPOSE]

PARTICIPATION

Participation is voluntary. You will not be retaliated against for declining to participate or for providing critical feedback.

CONFIDENTIALITY — SELECT AND CUSTOMIZE ONE

- Responses are **anonymous** and are not linked to your identity.
- Responses are **confidential** and will be reported only in groups.
- Responses are **pseudonymous** and may be connected to a unique survey identifier.
- Responses are **identifiable** to specified members of the organization.

Results for small groups may be suppressed or combined to reduce the possibility that individuals can be identified.

WHO WILL RECEIVE RESULTS

Aggregated results may be accessed by:

[LIST INTERNAL TEAMS, CONSULTANTS, DESIGNERS, HR PERSONNEL, OR OTHER RECIPIENTS]

INDIVIDUAL EMPLOYMENT DECISIONS

The Workplace Priorities App is not intended to make individual employment decisions. The organization will not use the app as the sole or determinative basis for hiring, termination, promotion, compensation, discipline, or individual performance evaluation.

MORE INFORMATION

For questions about the survey or the use of your information, contact:

[ORGANIZATION CONTACT]

For additional privacy information, see:

[LINK TO YOUR EMPLOYEE OR SURVEY PRIVACY NOTICE]

Privacy Notice

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

This Privacy Notice is referenced by Section 19 of the Business Terms of Service and by the order-of-precedence clause. It completes the set of documents the Terms incorporate.

1. Who we are

Workspace Design Magazine, LLC, a Virginia limited liability company doing business as “Work Design” (“Provider,” “Work Design,” “we,” “us,” or “our”), provides the Workplace Priorities App and related services (the “Service”). Our principal place of business is 904 N Lexington St., Arlington, VA 22205, United States.

2. Scope of this Notice

This Notice explains how we process Personal Data **in our role as an independent controller or business** — for example, information about the people who create and administer accounts, our billing contacts, visitors to our website, and people who contact us.

It does **not** govern the survey participant data that a customer submits to run an assessment. For that data the customer is the controller (or “business”) and we act as processor on the customer’s documented instructions; that processing is governed by the **Data Processing Addendum** and the customer’s own participant notice and privacy notice.

Capitalized terms not defined here have the meaning given in the Business Terms of Service.

3. Information we collect

3.1 Account Data

Information relating to an account, Authorized Users, billing contacts, transaction records, authentication information, and use of the Service.

3.2 Usage Data

Technical and operational information concerning the configuration, performance, security, and use of the Service, such as device and log information, IP address, and product-analytics events relating to our own business operations.

3.3 Website and marketing data

Information you provide through our website, forms, event sign-ups, and marketing communications, and information collected through cookies and similar technologies (see Section 11).

3.4 Communications

Records of your correspondence with us, including support requests and feedback.

We ask that account and billing contacts do **not** submit the categories of prohibited or Sensitive Data listed in Section 12 of the Business Terms of Service.

4. How we use information

We use Personal Data we control to:

- create, administer, and secure accounts and process payments;
- provide, maintain, support, and improve the Service;
- communicate about the Service, including service and security notices and, where permitted, marketing;
- produce Aggregated Data and generalized statistical findings that do not identify a customer or an individual;
- detect, prevent, and address fraud, abuse, and security incidents;
- comply with law and enforce our agreements; and
- establish, exercise, or defend legal claims.

5. AI and automated processing

The Service uses AI Components to analyze information and generate outputs. AI-generated outputs may be incomplete or inaccurate and are reviewed by appropriately qualified people before any material decision. We do **not** use the Service to make decisions producing legal or similarly significant effects about you without meaningful human involvement, and we do not use it for emotion recognition, biometric categorization, covert monitoring, or inference of protected characteristics. We do not use identifiable customer content or participant responses to train general-purpose AI models for unrelated customers without separate, express opt-in consent, and we configure third-party AI providers so that customer content is not used to train their general models.

6. Legal bases (EEA / UK)

Where the GDPR or UK GDPR applies to our own controller processing, we rely on: performance of a contract; our legitimate interests in operating, securing, and improving the Service and our business; compliance with legal obligations; and consent where required (for example, certain marketing or cookies). You may withdraw consent at any time without affecting prior processing.

7. How we share information

We share Personal Data with subprocessors that provide hosting, analytics, communications, payment processing, customer support, and AI functionality, under written agreements requiring appropriate protection. We publish a current list of material subprocessors at workdesign.co/legal/subprocessors. We may also share information to comply with law, enforce our agreements, protect rights and safety, and in connection with a merger, financing, or sale of assets. We do **not** sell Personal Data, and we do not share it for cross-context behavioral advertising, as those terms are defined under applicable U.S. state privacy laws.

8. International transfers

Where Personal Data is transferred from the European Economic Area, United Kingdom, or Switzerland to a country not recognized as providing adequate protection, we use an appropriate transfer mechanism, which may include the

European Commission's Standard Contractual Clauses, the UK International Data Transfer Agreement or Addendum, another approved mechanism, or an applicable adequacy decision.

9. Retention

We retain Personal Data for as long as necessary for the purposes described here, subject to legal-retention obligations, fraud and security requirements, dispute preservation, and ordinary backup cycles. Unless otherwise stated in an Order Form or account setting, we may retain identifiable Customer Content for 365 days after completion of a project. Deletion of Customer Content does not require deletion of Aggregated Data that no longer identifies a customer or an individual.

10. Security

We maintain a documented security program with administrative, technical, and physical safeguards designed to protect Personal Data against unauthorized access, acquisition, alteration, disclosure, loss, or destruction. No system is completely secure, and we cannot guarantee that a security incident will never occur.

11. Cookies and analytics

Our website uses cookies and similar technologies for essential functionality, preferences, and analytics. Where required by law, we request consent for non-essential cookies and provide controls to manage them.

12. Your rights

Depending on where you live, you may have rights to access, correct, delete, restrict, or object to processing of your Personal Data; to data portability; to withdraw consent; and to lodge a complaint with a supervisory authority or attorney general. We will not discriminate against you for exercising these rights. To make a request, contact us using Section 14. If we process data solely on a customer's behalf, we may refer your request to that customer.

13. Children

The Service is a business tool intended for adults. It is not directed to children, and we do not knowingly collect Personal Data from anyone under 18. Customers must not submit information concerning children under 18 through the Service.

14. How to contact us

Workspace Design Magazine, LLC (d/b/a Work Design)

904 N Lexington St.

Arlington, VA 22205

Email: bob.fox@workdesign.com

15. Changes to this Notice

We may update this Notice to reflect changes to the Service, the law, or our practices. We will provide reasonable notice of material changes and update the “Last updated” date above.

Privacy, Data & AI — Summary

HOW THE TOOL HANDLES DATA, AI, AND PEOPLE

Workplace Priorities is built for aggregate workplace planning and employee-experience research — never for decisions about identifiable individuals. The commitments below summarize the key privacy, data-protection, and AI provisions. The complete **Business Terms of Service**, **Privacy Notice**, **Data Processing Addendum**, **AI & Workplace-Use Acknowledgment**, and recommended **Participant Notice** are available in the Reference Guide.

AI is decision-support, not a decision-maker

The Service uses AI and automated analysis to generate summaries, scores, priorities, and recommendations. AI outputs can be incomplete or inaccurate and are reviewed by appropriately qualified people before any material decision. The tool is not a substitute for professional, legal, HR, design, or engineering judgment, and has no authority to make decisions on anyone's behalf.

Not for individual employment decisions

Results must never be the sole or determinative basis for hiring, termination, promotion, compensation, discipline, or individual performance evaluation. The Service does not perform emotion recognition, biometric categorization, covert monitoring, or inference of protected characteristics.

Anonymity described accurately

A survey is only called “anonymous” when responses genuinely cannot be associated with an identifiable participant; otherwise it is described as confidential, pseudonymous, or reported only in aggregate. Small groups are suppressed or combined to reduce the possibility of reidentification.

Reporting thresholds protect participants

Results may be suppressed or combined where a reporting group contains fewer than five completed responses, or where reporting could otherwise enable reidentification. These thresholds cannot be circumvented — and the cross-department alignment layer applies the same roughly five-respondent floor.

Clear data-protection roles

For participant lists and survey responses the customer is the controller (or “business”) and the provider acts as processor on the customer's documented instructions. A Data Processing Addendum governs that processing and is available in the Reference Guide.

Your content is not used to train general AI models

Identifiable customer content and participant responses are not used to train general-purpose AI models for other customers without separate, express opt-in consent. Third-party AI providers are configured so that customer content is

not used to train their general models. Only aggregated, de-identified, or identifier-stripped data is used to evaluate and improve the Service.

Aggregate-only, with no reidentification

Aggregated insights are combined and processed so they cannot reasonably identify a customer or an individual, and the provider does not attempt to reidentify properly de-identified data except to test that de-identification controls work.

Security, retention & deletion

The provider maintains a documented security program with administrative, technical, and physical safeguards, and honors project retention periods and customer-selected deletion, subject to routine backup cycles and legal requirements.

Sensitive data is minimized. Customers submit only information reasonably necessary for the workplace assessment and must not submit government identifiers, financial credentials, medical records, biometric templates, precise real-time geolocation, or information about children (under 18) — and special-category data is collected only where expressly supported and lawfully justified.