



WORK DESIGN

# Privacy, Data & AI

Plain-language summary

---

The key privacy, data-protection, and AI commitments at a glance. The binding detail lives in the Business Terms of Service, Privacy Notice, and Data Processing Addendum.

# 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.