Data Retention and Deletion Policy

PeopleMetrics, Inc. · July 2025 · External Version

This document is approved for sharing with clients, prospects, and vendors as part of security due diligence requests. It does not contain internal operational details. All content is proprietary and confidential to PeopleMetrics, Inc.

1. Purpose

This policy defines PeopleMetrics' approach to data retention and deletion, ensuring that data is preserved only for as long as necessary to meet business, contractual, or legal obligations. It supports ISO/IEC 27001:2022 compliance and minimizes the risk associated with retaining unnecessary or outdated information.

2. Scope

This policy applies to all client, respondent, and internal operational data stored by PeopleMetrics across all formats and storage locations, including databases, backups, cloud platforms, and shared drives. It applies to all employees, contractors, and vendors who manage or access company data. It governs both digital data and physical hardware disposal.

3. Retention Principles

PeopleMetrics retains data only as long as necessary to meet:

- Contractual obligations to clients, including multi-year reporting and benchmarking requirements.
- Legal and regulatory requirements.
- Legitimate business needs such as trend analysis and historical reporting.

Data access is governed by strict access control policies to prevent misuse of retained records.

4. Deletion and Minimization

- When data is no longer required for business, contractual, or legal purposes, it is securely deleted.
- Sensitive or personal data used for testing or development purposes is anonymized prior to use.
- Periodic reviews are conducted to assess whether continued retention of stored data is justified.

5. Hardware Disposal

When data-bearing hardware reaches end-of-life or is replaced, PeopleMetrics ensures all data is securely wiped in accordance with industry best practices prior to physical disposal. Where external vendors are engaged for physical destruction, a certificate of destruction or equivalent attestation is obtained.

6. Roles and Responsibilities

- **Information Security Officer::** Oversees retention practices and policy compliance.
- **Data Owners::** Ensure data under their control is reviewed for continued relevance.
- **IT/DevOps Team::** Supports secure storage, backup management, and deletion when requested.

7. Compliance and Review

This policy is reviewed annually or whenever significant changes occur in legal, contractual, or operational data requirements.

ISO 27001:2022 Certification · Certificate No. ISMS-PE-092325 · Issued by A-LIGN Compliance and Security, Inc. · Valid through September 23, 2028