Assessment conducted by: ComplyMe.AI
Reference ID: a049d713-651f-4ffd-8cdb-f3bff5914de7
Date of the report: 2026-11-17

Third Party Privacy Risk Assessment (Final)

This is a finalised privacy risk assessment based on submitted and independently researched information.

Third Party Organisation

- **Name:** Vendor
- **Domain:** Vendor.com

Categories of Data

- **Third Party Provided Summary:** The third party stated they process "all types of personal information" and that they are a "survey platform" using a digital platform to collect this information.
- **Independent Research Summary:** Vendor processes two distinct data streams. "Platform User Data" includes account administration information, billing, and contact details. "Respondent Data" (customer-defined) can include sensitive or special categories of personal information (health, political, ethnicity, biometrics) depending on the survey design.
- **Discrepancies/Gaps:** The third party response was extremely high-level and failed to differentiate between account user data and respondent-provided data. There is a discrepancy in depth; the third party's summary was insufficient compared to the actual operational reality identified in independent research.

Handling of Data

- **Third Party Provided Summary:** The third party stated, "we are a survey platform so use a digital platform to collect personal information."
- **Independent Research Summary:** Vendor operates as a data processor. Data is collected through customer-initiated surveys and integrations, processed according to customer instructions, stored in secure regionalized cloud environments, and can be deleted by customers using "one-touch" tools to support Data Subject Requests (DSRs).
- **Discrepancies/Gaps:** The third party response provided minimal operational detail. There is a significant gap in the provided information regarding storage lifecycle and deletion mechanisms, which were only clarified through independent research.

Data Subject Control

- **Third Party Provided Summary:** "We allow users to exercise their privacy rights through the platform tools."

SAMPLE REPORT - All Rights Reserved, ComplyMe.AI

- **Independent Research Summary:** Vendor provides specific technical capabilities for customers to honor data subject rights (access, modification, deletion). The organization notes that the responsibility for specific protections (like age-gating for minors) rests with the customer.
- **Discrepancies/Gaps:** No major discrepancy, though the third party failed to mention that the onus of compliance regarding specific groups (e.g., children) remains with the client rather than the platform.

Data Sovereignty

- **Third Party Provided Summary:** "We have data centre locations in Australia."
- **Independent Research Summary:** Vendor utilizes a global cloud infrastructure (AWS and others). They support regional residency to meet sovereignty requirements, but do not publicly map specific data centre locations for security reasons.
- **Discrepancies/Gaps:** The third party's claim is accurate but incomplete regarding their broader global hosting strategy.

Certifications

- **Third Party Provided Summary:** "We are compliant and certified with ISO27001."
- **Independent Research Summary:** Vendor holds a comprehensive list of certifications: SOC 2 Type II, ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 42001, FedRAMP High, HITRUST, and IRAP.
- **Discrepancies/Gaps:** The third party significantly understated their security posture by only mentioning ISO27001, when their actual portfolio is much more extensive.

Information Security Practices

- **Third Party Provided Summary:** Information not provided.
- **Independent Research Summary:** Vendor employs encryption (transit/at-rest), RBAC/SSO, regular independent penetration testing, continuous vulnerability scanning, high-availability architecture, and sensitive data redaction policies.
- **Discrepancies/Gaps:** There is a significant gap here, as the third party failed to provide any information on their security controls, forcing reliance on external research.

Legal

- **Third Party Provided Summary:** "You can find legal/contractual terms on our website."
- **Independent Research Summary:** Vendor uses a standard legal framework, including DPAs, SCCs, UK Addendum, and MSAs. They explicitly state they do not provide legal advice, placing compliance responsibility on the customer.
- **Discrepancies/Gaps:** The third party provided no detail or context in their response, necessitating independent research to verify the existence of standard data protection frameworks.

SAMPLE REPORT - All Rights Reserved, Complyvie AI

Data Breaches

- **Third Party Provided Summary:** “No data breaches.”
- **Independent Research Summary:** No systemic infrastructure breaches are evident. However, there was an incident in October 2026 involving a compromised Vendor account at a university due to phishing and legacy login exploitation, rather than a platform-level breach.
- **Discrepancies/Gaps:** The third party’s response is technically correct regarding a platform breach, but lacks the necessary nuance regarding account-level security incidents that impact their services.

Potential Gaps

- **APP 3 (Collection of solicited personal information):** As a data processor, Vendor collects what its customers (the controllers) ask it to collect. A potential gap exists if the third party does not provide adequate guidance or guardrails to customers regarding the “reasonableness” and “necessity” of the sensitive information being collected via their platform.
- **APP 5 (Notification of the collection of personal information):** Vendor relies on its customers to provide the required notices to individuals. The third party does not appear to provide integrated, automated notification tools for its customers to ensure they meet APP 5 requirements when they configure surveys.
- **APP 6 (Use or disclosure of personal information):** Vendor must ensure that respondent data is only used for the purposes defined by the customer. The third party appears to meet this through platform tools, but the gap remains in verifying that customers do not use respondent data in ways that contradict the original purpose of collection.
- **APP 8 (Cross-border disclosure):** Vendor processes data globally. While they utilize SCCs and DPAs, the third party response provided no assurance regarding how they manage cross-border transfer requirements specifically for Australian entities, despite the clear legal framework for cross-border disclosures.
- **APP 11 (Security of personal information):** The third party has a very high security posture (SOC2, ISO, etc.). However, the failure to provide any security practice information in the response phase is a procedural gap. They rely heavily on the customer to correctly configure the security settings of their instances.

Overall Risk Assessment

Risk Rating: MEDIUM

Explanation: The risk is rated as MEDIUM. While independent research confirms that Vendor maintains a robust security posture with numerous high-level certifications and clear contractual frameworks (DPA/SCCs), there is a significant discrepancy between the actual maturity of the organization and the poor quality of the information provided by the third party in their survey response. The third party provided minimal, high-level answers that were often factually incomplete (e.g., regarding certifications) or entirely

SAMPLE REPORT - All Rights Reserved, CompMe.AI

omitted (e.g., regarding security practices). This forces a heavy reliance on independent research to verify their claims and creates a concern regarding the third party's internal processes for vendor risk assessment and transparency. While they are likely a safe vendor to rely on, the lack of transparency in the initial response process represents an operational gap that must be addressed through direct contractual due diligence.

Appendix - Independent Research

Privacy Research Report: Vendor

Date: November 17, 2026
Subject: Privacy and Security Assessment of Vendor (Vendor.com)
Role: Privacy Analyst

---

1. Data Handling and Categories

Vendor acts primarily as a **data processor** for its customers. The data handled is categorized into two distinct streams:

- **Platform User Data (Account/Business Data):** Information provided by Vendor customers (e.g., account administrators) to access the platform. This includes contact details (name, email, phone number), billing/financial information, and marketing preferences.
- **Respondent Data (Survey/Project Data):** Information collected by customers using the Vendor XM Platform. Vendor does not define or restrict the *types* of data a customer may collect via their surveys. Consequently, this can include **sensitive and special categories of personal information** (e.g., health data, political opinions, ethnicity, or biometric data), depending entirely on the survey questions designed by the customer.

2. Collection, Usage, Storage, and Deletion

Vendor manages data according to the "Controller-Processor" model:

- **Collection:** Data is collected through customer-initiated surveys, integrations, and platform usage.
- **Usage:** Vendor processes this data strictly as instructed by its customers to provide the platform's functionality (e.g., survey distribution, analytics).
- **Storage:** Data is stored in secure, regionalized cloud environments.
- **Deletion:** Vendor provides administrative tools for customers to manage Data Subject Requests (DSRs), including "one-touch" data deletion features to comply with rights to erasure under regulations like GDPR and CCPA. Customers retain control over retention policies.

SAMPLE REPORT - All Rights Reserved, ComplyMe.AI

3. Data Subject Control and Protections

- **Data Subject Control:** Vendor provides technical capabilities for customers to honor data subject rights, such as data access, modification, and deletion.
- **Children/Vulnerable Groups:** Vendor does not implement specific age-gating for all surveys by default; responsibility for compliance with laws protecting children (e.g., COPPA) rests with the customer creating the survey.
- **Compliance Schemes:** Vendor aligns its operations with major frameworks, including GDPR and CCPA. The organization maintains robust transparency regarding its role as a processor and facilitates compliance for its users through its platform tools.

4. Datacenter and Hosting Locations

Vendor utilizes a global infrastructure strategy. * **Hosting:** The platform leverages major cloud service providers, including Amazon Web Services (AWS) and other enterprise-grade, SSAE-18 audited data centers. * **Residency:** Vendor supports regional data residency, allowing customers to host and process data within specific geographic regions (e.g., EU, US) to meet local data sovereignty requirements. Specific datacenter locations are generally disclosed to customers via support channels rather than public mapping for security reasons.

5. Information Security Standards and Certifications

Vendor maintains an extensive portfolio of independent security certifications: * **SOC 2 Type II:** Validates security, availability, and confidentiality. * **ISO Certifications:** ISO 27001 (Information Security), ISO 27017 (Cloud Security), ISO 27018 (Cloud Privacy), ISO 27701 (Privacy Information Management), and ISO 42001 (AI Governance). * **FedRAMP:** Authorized at the "High" impact level for U.S. federal agency usage. * **HITRUST:** Certified, confirming compliance with rigorous healthcare and HIPAA standards. * **IRAP:** Assessed against the Australian Information Security Manual (ISM).

6. Information Security Practices and Controls

To ensure the CIA (Confidentiality, Integrity, Availability) triad, Vendor employs: * **Confidentiality:** Data encryption in transit (TLS) and at rest; access is restricted via Role-Based Access Control (RBAC) and Single Sign-On (SSO). * **Integrity:** Regular penetration testing (independent third-party) and continuous vulnerability scanning. * **Availability:** High-availability architecture with quick failover points, redundant hardware, and daily backups. * **Sensitive Data Handling:** Customers can implement "Sensitive Data Policies" to automatically flag or redact PII/sensitive data within the platform.

7. Legal and Contractual Terms

Vendor utilizes a standardized legal framework for privacy and data protection: * **Data Processing Addendum (DPA):** Includes Standard Contractual Clauses (SCCs) and the UK Addendum to legitimize international data transfers. * **Master Services Agreements (MSA):** Sets the base legal terms, often supplemented by region-specific

SAMPLE REPORT. All Rights Reserved. ComplyMe.AI

amendments or General Terms and Conditions (GTC). * **Responsibility Disclaimer:** Vendor explicitly notes that while it provides the *technology* to enable compliance, it does not provide legal advice; customers remain responsible for their own regulatory compliance.

8. Data Breaches and Security Concerns

- **General Posture:** Vendor maintains a strong security reputation, with no evidence of systemic, large-scale breaches of its core infrastructure.
- **Recent Incident:** In October 2026, a security incident was reported involving a compromised Vendor account at The Ohio State University. This was not a breach of the Vendor platform itself, but rather an unauthorized access event where a legacy, non-SSO login method was exploited to distribute phishing messages. Vendor cooperated with the university to investigate, highlighting the importance of enforcing modern authentication (SSO) and robust account management.

Sources

- Vendor, “Data Protection & Privacy,” URL
- Vendor, “Privacy Statement,” April 23, 2026, URL
- Vendor, “Sensitive Data Policy,” URL
- Vendor, “Vendor Security and Privacy Accreditations,” URL
- Vendor, “Data Security & Privacy for Digital Experience Analytics,” URL
- Vendor, “Vendor’ commitment to secure and private AI,” August 06, 2024, URL
- Vendor, “Contractor Data Processing Agreement (CDPA),” March 15, 2024, URL
- Vendor, “Standard Contractual Clauses Update,” URL
- Vendor, “Security Statement,” June 10, 2024, URL
- Vendor, “Vendor Security and Compliance,” URL
- Vendor, “Vendor Subprocessors,” URL
- The Ohio State University, “Security Incident Involving Vendor Account,” October 08/09, 2026, URL

SAMPLE REPORT - All Rights Reserved, Complyvie.AI