PERMASTEELISA GROUP

DATA TRANSFER RISK ASSESSMENT (DTRA) – MIDDLE EAST

Date of Assessment: October 2026

Assessment Scope: Transfer of Employee HR and Demographic Data for Global Engagement Survey

Data Exporter: Permasteelisa Group (Middle East Entities, including UAE and Kingdom of Saudi Arabia)

Data Importer: McLean & Company ("Survey Provider")

1. TRANSFER CONTEXT AND DATA CHARACTERISTICS

This Data Transfer Risk Assessment evaluates the compliance, risks, and safeguards associated with transferring employment metadata from Permasteelisa Group's Middle Eastern entities to an external data processor (McLean) hosted outside the Gulf Cooperation Council (GCC) region.

Category	Details
Data Categories Transferred	Employee ID, Company Email, Country, Region, Location, Legal Entity, Department, Cost Center, Position Title, Retail/Curtain Wall status, White/Blue-Collar status, Leader, Direct Report, Generation, Gender.
Special Categories (Sensitive Data)	None. Personal email addresses are excluded. No biometric, health, or religious data is processed.
Data Importer Location	United States of America (USA)
Transfer Mechanism	Standard Contractual Clauses (SCCs) alongside local supplementary contractual safeguards.

2. REGULATORY FRAMEWORK ANALYSIS

The transfer is subject to strict local privacy regulations in the Middle East, which require the Data Exporter to ensure that exported data receives protection equivalent to local standards.

2.1 Kingdom of Saudi Arabia (KSA PDPL)

Under Article 29 of the KSA Personal Data Protection Law (promulgated by Royal Decree No. M/19, fully enforced), cross-border transfers are permitted if they do not prejudice national security, are limited to the minimum amount of data necessary, and the destination country offers an adequate level of protection. If the destination lacks formal adequacy, appropriate safeguards (such as binding contractual clauses) and a specific risk assessment must be applied. This transfer complies by strictly minimizing the data to non-sensitive HR metadata required solely for statistical aggregation.

2.2 United Arab Emirates (UAE PDPL)

Articles 22 and 23 of the UAE Federal Decree-Law No. 45 of 2021 govern cross-border data transfers. Similar to the KSA PDPL and the EU GDPR, transfers to non-adequate jurisdictions require the execution of Standard Contractual Clauses or an equivalent legal instrument that binds the Importer to UAE-level data protection standards. Voluntary participation by the employee also serves to mitigate processing friction.

3. THREAT AND VULNERABILITY ASSESSMENT

We have assessed the likelihood and severity of potential risks associated with transferring data to the United States:

- **Foreign Authority Access (US Surveillance Laws):** Because the data is hosted in the USA, it theoretically falls under the jurisdiction of US laws like FISA Section 702 or the CLOUD Act. Mitigation: The data consists purely of corporate metadata for an internal HR engagement survey. It is highly improbable that this data would be of any interest to US national security or law enforcement agencies. Individual survey responses are decoupled from identifiers, neutralizing the risk.
- **Data Breach in Transit or at Rest (Low Risk):** Interception during the international transfer over public networks. Mitigation: Handled via mandated end-to-end encryption.
- **Re-identification Risk (High without mitigations, Low with mitigations):** The risk that Middle Eastern employees could be uniquely identified by their survey answers, leading to local workplace repercussions. Mitigation: Automated thresholds enforced by the Importer.

4. SUPPLEMENTARY SAFEGUARDS IMPLEMENTED

To ensure the data is protected to the standard required by KSA and UAE authorities, Permasteelisa Group and McLean have implemented the following binding safeguards:

Safeguard Type	Description & Implementation
Contractual	Execution of a comprehensive Data Processing Agreement (DPA) incorporating standard contractual clauses. The Importer is legally prohibited from using the data for secondary purposes, marketing, or independent analytics.
Organizational (Thresholds)	McLean enforces strict reporting limits: a minimum of 4 completed responses is required to display demographic-level quantitative data. A minimum of 8 responses is required to display free-text qualitative comments per department. Smaller groupings are automatically aggregated into "undefined" categories.
Technical (Encryption & Access)	All data transferred across borders is encrypted in transit (TLS 1.2/1.3) and at rest (AES-256). Permasteelisa management has zero access to individual response payloads.
Data Minimization & Deletion	No raw data or individual responses are shared back to Permasteelisa Group. McLean must irreversibly delete or permanently anonymize all identifiable records immediately following the conclusion of the survey reporting cycle.

5. CONCLUSION AND APPROVAL

Based on the technical, organizational, and contractual measures implemented, the risk of transferring the specified employee demographic data to the United States is deemed low and acceptable. The safeguards provided by McLean adequately address the requirements of the UAE PDPL and the KSA PDPL for cross-border transfers.