SaaS Jurisdictional Exposure Assessment

Prepared for: [Client Organization — Redacted] · Assessment Date: [Redacted] · Ref: HS-2026-00X

CONFIDENTIAL

01 · ENVIRONMENT SUMMARY

Parameter	Documented Value
Total SaaS tools assessed	24
Unique vendors identified	21
Vendors with U.S. parent entity	14 (66.7%)
Cross-border data transfer pathways identified	9
App-to-app integrations mapped	31
Tools with no documented data processing agreement	7
Assessment methodology	HarbourScan Framework v1.2 — Law 25 / PIPEDA / Cloud Act

02 · SAAS INVENTORY SNAPSHOT (8 OF 24 TOOLS SHOWN)

Tool / Service	Vendor Entity	Jurisdiction	U.S. Parent	Cloud Act	DPA Status
[Tool A — Collaboration]	[Vendor A — US parent]	United States	Yes	Confirmed	Not documented
[Tool B — CRM]	[Vendor B — US parent]	United States	Yes	Confirmed	Standard terms
[Tool C — File Storage]	[Vendor C — CA entity]	Canada	No	Not applicable	Documented
[Tool D — HR Platform]	[Vendor D — US parent]	United States	Yes	Confirmed	Not documented
[Tool E — Legal Mgmt]	[Vendor E — CA entity]	Canada	No	Low	Documented
[Tool F — Analytics]	[Vendor F — US parent]	United States	Yes	Confirmed	Not documented
[Tool G — Automation]	[Vendor G — US parent]	United States	Yes	High	Not documented
[Tool H — Communication]	[Vendor H — CA entity]	Canada	No	Not applicable	Partial

Note: Full inventory of 24 tools provided in complete assessment deliverable. Vendor names redacted in this preview.

03 · JURISDICTIONAL EXPOSURE FINDINGS

Finding 01

HIGH

Cloud Act Jurisdictional Exposure — 14 tools

14 of 24 assessed tools are operated by vendors with a U.S. parent entity, subjecting associated data to potential disclosure under the U.S. CLOUD Act (18 U.S.C. § 2523) regardless of where data is physically stored. Affected tools include core collaboration, CRM, HR, and workflow automation platforms.

Finding 02

HIGH

Undocumented Cross-Border Data Transfers — 9 pathways

Nine identified data transfer pathways to non-Canadian jurisdictions lack documented transfer impact assessments or contractual safeguards as required under Law 25, s. 17. The organization has not completed the mandatory cross-border transfer documentation required prior to disclosure of personal information outside Quebec.

Finding 03

MEDIUM

App-to-App Integration Data Flows — 31 pathways identified

Automated integration flows route personal information between platforms without documented review. Several pathways route data to U.S.-jurisdictional endpoints through intermediate automation tools, creating indirect Cloud Act exposure not captured by direct vendor assessment alone.

Finding 04

MEDIUM

Absence of Data Processing Agreements — 7 vendors

Seven vendors processing personal information on behalf of the organization operate without a documented data processing agreement or equivalent contractual instrument. This creates accountability gaps under Law 25, s. 18.3 and PIPEDA Principle 4.1.3.

04 · INTEGRATION DATA-FLOW RISK NOTES

Integration Pathway	Data Categories in Scope	Destination	Classification
[Tool A] → [Tool G] (automated sync)	Contact records, communication logs	United States	Jurisdictional Exposure
[Tool B] → [Tool F] (analytics pipeline)	Customer PII, behavioural data	United States	Jurisdictional Exposure
[Tool D] → [Tool A] (HR ↔ Collaboration)	Employee records, org structure	United States	Jurisdictional Exposure
[Tool C] → [Tool G] (file trigger)	Document metadata	United States	Review Required
[Tool E] → [Tool B] (legal ↔ CRM sync)	Matter identifiers, contact data	Canada	Low — Documented

01 **Complete Transfer Impact Assessments (TIAs)**

Law 25, s. 17 requires a TIA prior to disclosure of personal information outside Quebec. Assessments must be completed for all 9 identified cross-border transfer pathways. Template documentation provided in Annex B of the complete assessment deliverable.

02 **Execute Data Processing Agreements with 7 identified vendors**

Contractual instruments must be in place for all vendors processing personal information on behalf of the organization. Standard DPA template aligned to Law 25 and PIPEDA requirements provided in Annex C.

03 **Update Privacy Policy and Governance Documentation**

Law 25 requires publication of a governance policy identifying systems, applications, and third parties through which personal information transits. Current documentation does not reflect the 24-tool SaaS environment assessed.

04 **Establish a Quarterly Integration Audit Process**

App-to-app integrations change without requiring IT approval in most SaaS environments. A quarterly review process is recommended to maintain an accurate picture of data-flow pathways and ensure ongoing compliance documentation.