Sovereign Shift

US Cloud Dependency Audit

Prepared for

Veldstra Finance B.V.

Amsterdam, Netherlands · B2B Fintech, Expense Management SaaS

Report date: 2026-02-21
Engagement: Micro Team Audit
Turnaround: 2 weeks

This report contains regulatory analysis but does not constitute legal advice.
Legal obligations depend on entity classification, sector, and jurisdiction. Consult qualified counsel.

Document Control

Version	Date	Description
1.0	2026-02-21	Final report delivered to client

Distribution List

Name	Role	Access
Daan van der Berg	CEO	Full report
Marloes de Vries	CTO	Full report

Contents

Reader Guide

Section	CEO	CTO / IT	Operations	Legal
1. Executive Summary	●	●	●	●
2. Methodology	○	●		●
3. Dependency Landscape	○	●	●	○
4. Sovereignty & Risk	●	●	○	●
5. Replacement Analysis	○	●	●	○
6. Roadmap & Action Plan	●	●	●	○
7. Appendices		●		●

● = Primary audience · ○ = Optional/skim. Each section also shows its audience and key question at the top.

Executive Summary

For: Everyone.

Key question: What do we depend on, what's risky, what moves first?

1.1 Engagement Overview

Sovereign Shift was engaged by Veldstra Finance B.V. to conduct a US cloud dependency audit covering all SaaS tools, cloud services, identity providers, and integrations used by the organisation's 8 employees. The engagement ran from 2026-02-10 to 2026-02-21 and included admin console review, DNS analysis, SSO audit, integration inventory, and a stakeholder interview with the CTO.

This audit includes: dependency mapping, sovereignty and lock-in scoring, risk register, replacement short-list, and a sequenced migration plan with prerequisites and cost comparison. Migration execution (hands-on cutover) is a separate engagement.

1.2 Decision Page

Dependency	Verdict	Why	Effort
Google Workspace	Move next	Identity backbone for 6 services. Migrate only after standalone IdP deployed and email/calendar pilot validated.	medium
Slack	Move next	High US exposure, low lock-in, but workflow retraining needed. Move after quick-win tools are settled.	easy
GitHub	Move next	Controls deployment pipeline via Vercel. CI/CD rewrite required; needs planning, not a quick swap.	medium
Notion	Move now	Low criticality, no integrations that block other migrations. Markdown export available. Drop-in replacement.	easy
Figma	Move next	Design workflows are habit-heavy. Penpot has real gaps in prototyping. Move after team has bandwidth.	easy
Linear	Move now	Low lock-in, CSV export available, no critical integrations. Clean swap.	easy
Vercel	Move next	Depends on GitHub for deployment triggers. Move after GitHub → GitLab migration completes.	easy
Stripe	Leave alone	Critical revenue path with deep API coupling (Connect, Subscriptions, Invoicing). No clean alternative. Begin evaluation only.	hard
AWS (S3 + CloudFront)	Move next	S3-compatible API makes migration straightforward. Move alongside Vercel/GitHub in Phase 2.	medium
Intercom	Move now	Customer PII in US jurisdiction with no EU residency. Crisp is a drop-in EU alternative. Highest-priority quick win.	easy
HubSpot	Move next	Contains prospect/customer PII. EU hosting available on current plan, but US parent. Move in Phase 2 alongside other data-heavy services.	medium
1Password	Move now	Credentials vault in Five Eyes jurisdiction. Proton Pass is E2E encrypted, Swiss-hosted, direct import supported.	easy
Zoom	Move now	Used only for external calls. No lock-in, no data at rest. Free EU alternative available immediately.	easy
Sentry	Move now	Low criticality, Sentry SDK-compatible drop-in exists. Open-source, self-hostable.	easy
PostHog	Evaluate later	Already on EU Cloud (Frankfurt). Self-host option exists. No viable full-feature EU alternative. Revisit when Plausible adds product analytics.	easy

Move now = drop-in EU alternative, days of effort. **Move next** = viable alternative, weeks of planned work. **Evaluate later** = current setup acceptable, revisit when options mature. **Leave alone (for now)** = deep coupling, no clean alternative yet.

1.3 Key Numbers

14/15
dependencies controlled by US-headquartered companies

4
critical dependencies where disruption = operational halt

14/15
dependencies rated Easy or Medium to replace

6
services that can be moved within days ("Move now")

−€3,900/yr
estimated net annual savings after migration (incl. hosting)

1.4 Top Findings

1. CRITICAL **Google Workspace is a single point of failure.** It serves as the identity provider (SSO) for 6 other services. Loss of the Google account = lockout from Slack, Figma, Linear, Intercom, Notion, and Sentry simultaneously. (Observed)
2. CRITICAL **93% of dependencies are US-controlled** (14 of 15 services). The organisation has near-total dependency on US infrastructure subject to the CLOUD Act.[1] (Legal exposure)
3. MAJOR **Customer PII sits in US-hosted services.** Intercom (customer support) and Slack (internal messages) have no EU data residency on current plans. (Observed)
4. MAJOR **Stripe is deeply embedded and hard to replace.** The product is built on Stripe Connect, Subscriptions, and Invoicing. Migration to Mollie/Adyen would require significant API rework. (Observed)
5. MODERATE **Three unrecognised OAuth grants** in Google Workspace admin console, potentially exposing data to unaudited third parties. (Observed)
6. MODERATE **No documented exit strategy** for any current vendor. Contract renewal dates not centrally tracked. (Observed)

1.5 Strategic Recommendations

1. **Begin identity decoupling immediately.** Document all SSO dependencies (Phase 0), pilot a standalone EU identity provider for new services (Phase 1), complete full cutover after email migration (Phase 3). This is the highest-leverage action because it eliminates the single-point-of-failure risk.
2. **Migrate email and storage after pilot.** Proton for Business (email/calendar) and managed Nextcloud (file storage/docs). These are the most data-sensitive services with mature EU alternatives. Pilot with 2 users first.
3. **Replace US-hosted customer-facing tools immediately.** Intercom → Crisp and Zoom → Jitsi are quick wins that remove customer PII from US jurisdiction within days.

[1] Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2713 (2018).

4. **Begin evaluating Stripe alternatives now.** Even if migration is 6–12 months away, understanding the Mollie/Adyen API gap early preserves optionality.
5. **Establish a vendor sovereignty policy.** Require EU data residency and documented exit strategy for all new tool procurement.

1.6 What Happens If You Do Nothing

If no action is taken, Veldstra Finance remains fully dependent on US-controlled infrastructure. A single regulatory event (invalidation of the EU-US Data Privacy Framework, a CLOUD Act data request, or a vendor policy change) could disrupt operations with no fallback.

Under GDPR Article 83, fines for inadequate international transfer safeguards may reach €20M or 4% of annual turnover, whichever is higher.[2] For a fintech whose customers increasingly require documented exit strategies from their suppliers, unaddressed dependency is also a commercial risk: lost deals from enterprises that will not accept the exposure.

[2] GDPR Art. 83(5)(c). Actual exposure depends on supervisory authority enforcement priorities and entity classification. This is not a prediction of fine amount.

Methodology

For: CTO, compliance, legal

Key question: How was this audit conducted and how should I interpret the scores?

2.1 Audit Framework

This audit examines technology dependencies across three layers:

- **Infrastructure layer:** cloud providers, DNS, CDN, compute, storage
- **Platform layer:** identity providers, CI/CD, databases, payment processing
- **Application layer:** SaaS tools for communication, collaboration, productivity

Every finding is classified using an evidence label:

Label	Meaning
Observed	Verified through direct inspection (admin console, API, DNS, SSO logs)
Legal exposure	Risk exists by operation of law (statute, regulation, court precedent). Not a prediction of enforcement.
Inferred	Deduced from documentation, interviews, or traffic analysis. Confidence: High/Medium/Low
Unknown	Gap identified but not resolvable within engagement scope

Frameworks referenced: EU Cloud Sovereignty Framework (SEAL 0–4)[3], CIGREF Trusted Cloud Referential v2, DORA[4] (Regulation (EU) 2022/2554), GDPR Chapter V[5].

2.2 Data Collection

Method	What was examined
Admin console review	Google Workspace admin, connected OAuth apps, user directory
DNS & MX record analysis	MX, SPF, DKIM, DMARC, CNAME records for primary domain
SSO/IdP configuration	Google SSO connections, SAML/OAuth grants to third-party apps

[3]European Commission, "European Cloud Sovereignty Framework" (2025).
[4]Regulation (EU) 2022/2554, Digital Operational Resilience Act.
[5]Regulation (EU) 2016/679, Articles 44–50.

Method	What was examined
Stakeholder interview	1 interview with CTO (60 min) covering stack, pain points, priorities
Integration & API inventory	OAuth apps list, webhook configurations, API key usage
Shadow IT check	Unrecognised OAuth grants in Google Workspace; DNS subdomain scan

Network traffic analysis and contract review were not performed. Neither was warranted for an 8-person team on month-to-month SaaS subscriptions.

2.3 Scoring

Sovereignty Score (per dependency, 0–4 scale, based on EU Cloud Sovereignty Framework SEAL levels). Per-dimension breakdown in Appendix B.

4/4	Full EU	EU-owned, governed, hosted, EU jurisdiction only, open-source or open standards
3/4	High	EU-hosted and EU-jurisdiction, but non-EU parent company, or non-EU country with adequacy decision (CH, UK)
2/4	Moderate	EU data residency offered, but subject to non-EU extraterritorial law (e.g., CLOUD Act via parent)
1/4	Low	Non-EU controlled, some EU compliance measures in place (SCCs, DPA)
0/4	None	Fully non-EU controlled, no EU data residency, subject to foreign government access

Note: Switzerland (CH) and the United Kingdom (UK) have EU adequacy decisions but are not EU/EEA member states. Services headquartered in CH or UK score 3/4 (not 4/4) unless self-hosted on EU infrastructure. Open-source self-hosted services score based on the hosting jurisdiction, not the project origin.

Replaceability: Easy / Medium / Hard / Do Not Touch Yet.

Feature fit: High / Adequate / Gaps / Poor, with specific gap callouts. No percentages.

2.4 Limitations

- Scope limited to SaaS and cloud services. On-premise hardware not assessed.
- Network traffic analysis not performed (not required for this engagement size).
- Financial data accuracy depends on information provided during interview.
- Shadow IT discovery limited to OAuth audit and DNS scan.
- This report contains regulatory analysis but does not constitute legal advice. Legal obligations depend on entity classification, sector, and jurisdiction.

Dependency Landscape

For: CTO, IT, operations

Key question: What do we depend on, who controls it, and what are the integration relationships?

3.1 Dependency Inventory

15 dependencies identified across 11 categories. The compact table below shows the decision-relevant view; full vendor, renewal, auth, data-type, and integration fields are delivered as CSV.

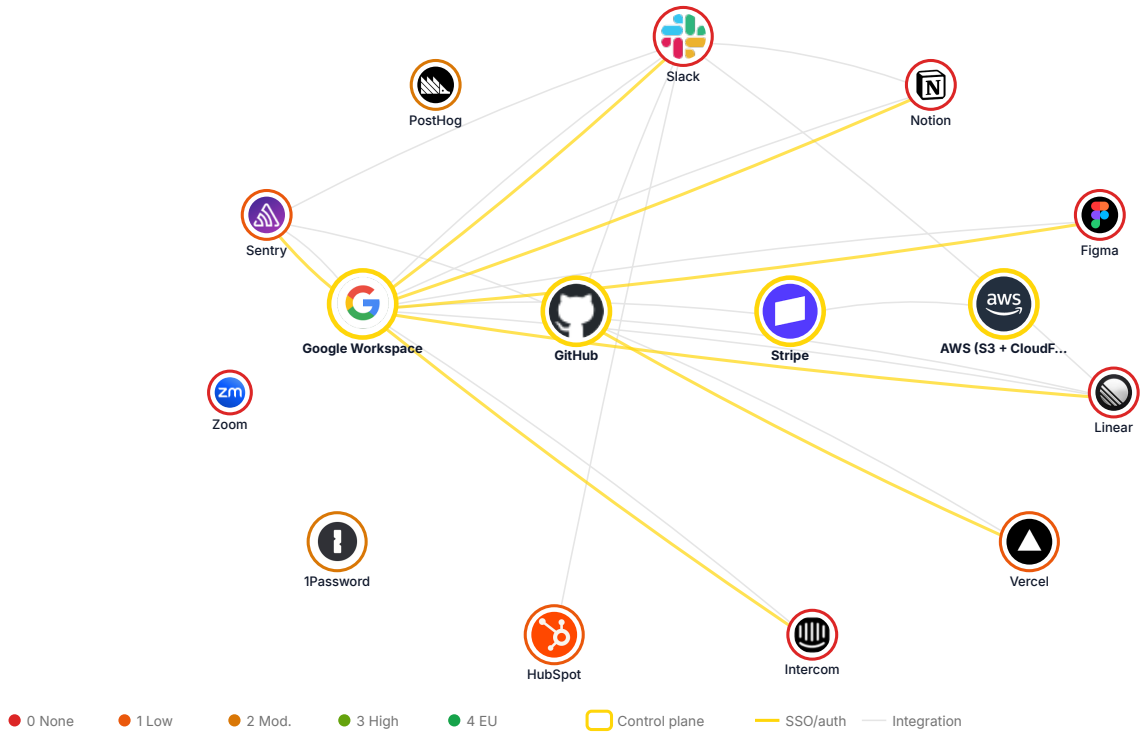
Service / vendor	Category	HQ	Sov.	Replaceability	Criticality
Google Workspace Google LLC	Email/docs	US	1/4	Medium	Critical
Slack Salesforce Inc.	Messaging	US	0/4	Easy	High
GitHub Microsoft Corp.	Source/CI	US	0/4	Medium	Critical
Notion Notion Labs Inc.	Docs/wiki	US	0/4	Easy	Medium
Figma Figma Inc.	Design	US	0/4	Easy	Medium
Linear Linear Orbit Inc.	Project Management	US	0/4	Easy	Medium
Vercel Vercel Inc.	Hosting	US	1/4	Easy	High
Stripe Stripe Inc.	Payment Processing	US	2/4	Hard	Critical
AWS (S3 + CloudFront) Amazon Web Services	Cloud infra	US	1/4	Medium	Critical
Intercom Intercom Inc.	Support	US	0/4	Easy	Medium
HubSpot HubSpot Inc.	CRM	US	1/4	Medium	High
1Password AgileBits Inc.	Passwords	CA	2/4	Easy	High
Zoom Zoom Video Communications	Video	US	0/4	Easy	Low
Sentry Functional Software Inc.	Errors	US	1/4	Easy	Medium
PostHog PostHog Inc.	Analytics	US	2/4	Easy	Medium

All inventory rows are Observed. Full evidence basis, renewal dates, auth methods, data types, and integration fields are delivered as CSV.

Sovereignty: 0/4 *None ·* 1/4 *Low ·* 2/4 *Moderate ·* 3/4 *High ·* 4/4 *Full EU · Replaceability:* 🟢 *Easy ·* 🟡 *Medium ·* 🟠 *Hard ·* 🔴 *DNT · See §2.3.*

3.2 Dependency Network Graph

Node size indicates business criticality. Colour indicates sovereignty score (red = low, green = high). Gold borders highlight control-plane services.



Key observation: Google Workspace sits at the centre, acting as the identity provider for 6 other services. This is the single largest concentration risk.

3.3 Jurisdiction Exposure

14 services are US-headquartered and may be subject to the US CLOUD Act.[6] 1 is Canadian (Five Eyes). 5 offer EU data residency, but parent companies remain US-incorporated.

Jurisdiction	Services	Legal exposure
United States (CLOUD Act, FISA 702)	14 services	US authorities may compel data disclosure regardless of storage location.
Canada (Five Eyes)	1 (1Password)	MLAT cooperation with US. Lower direct risk but not EU-sovereign.
EU data residency offered	5 services	Google, Stripe, AWS, HubSpot, PostHog offer EU storage. CLOUD Act still applies via parent company.

3.4 Vendor Concentration

Google controls 1 service but it is the identity backbone for 6 others. Microsoft (via GitHub) controls the entire software delivery pipeline. **Single-point-of-failure count: 3** (Google Workspace, GitHub, Stripe).

3.5 Control-Plane Analysis

A control plane is a service that other services depend on for authentication, deployment, or operation. Loss cascades to all dependent services.

Control plane	What it controls	Cascade impact
Google Workspace (IdP)	Slack, Figma, Linear, Intercom, Notion, Sentry	Lockout from 6 services simultaneously
GitHub	Vercel (deployment)	Cannot deploy code changes
Stripe	Payment processing	Cannot process payments or issue invoices
AWS	File storage, CDN, serverless	Product outage for end customers

3.6 Shadow IT

The Google Workspace OAuth audit revealed **3 unrecognised app grants**: (Observed)

1. Chrome grammar extension with full Gmail read access

[6] CLOUD Act, 18 U.S.C. § 2713. Whether a specific data request occurs depends on law enforcement interest, but the legal authority exists regardless of data storage location.

2. Expired calendar scheduling tool with read/write permissions
3. File conversion service with Google Drive read access

Recommendation: Revoke all three immediately. Require CTO approval for new OAuth grants.

Sovereignty & Risk Assessment

For: CEO, board, legal, compliance

Key question: How exposed are we, and which risks should we act on first?

4.1 Sovereignty Scores

The organisation's sovereignty posture is weak across all dimensions. Per-dependency scores are in the inventory table (Section 3.1). The per-dimension breakdown is in Appendix B.

Weakest dimensions:

- **Strategic sovereignty:** near-total reliance on US-owned companies (14 of 15 score 0)
- **Supply chain sovereignty:** no visibility into vendors' upstream dependencies

Relative strengths:

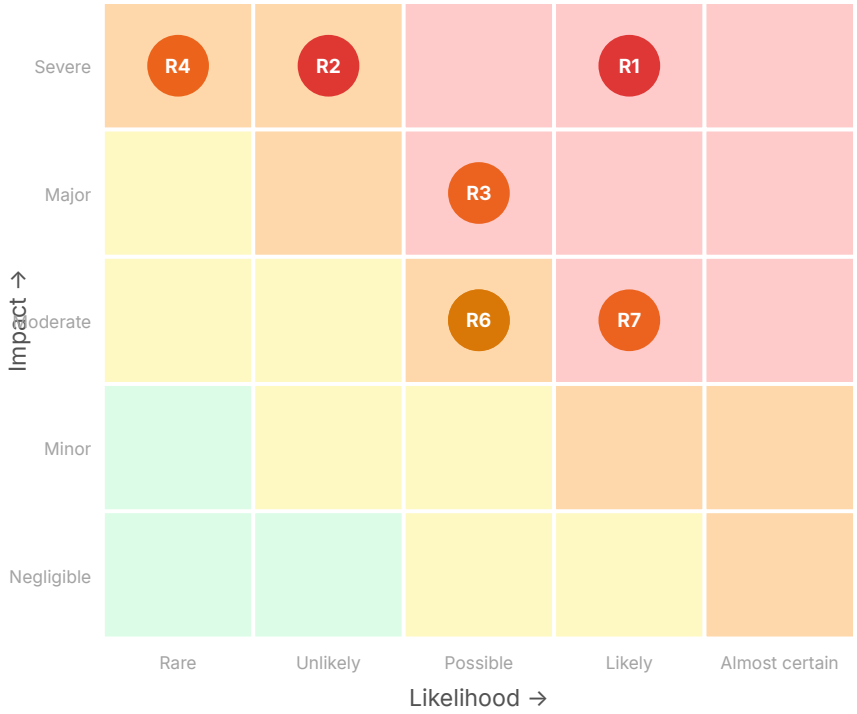
- **Data sovereignty:** 5 services offer EU data residency (though this may not protect against CLOUD Act requests via the corporate parent)
- **Technology sovereignty:** some services use open standards (Git, CalDAV, S3 API)

4.2 Risk Register

ID	Risk	Category	L	I	Sev.	Ev.
R-01	US government access to customer financial data via CLOUD Act	Legal / Jurisdictional	4/5	5/5	Critical	Legal exposure
R-02	Google Workspace outage or account suspension causes total operational halt	Operational / Concentration	2/5	5/5	Critical	Observed
R-03	EU-US Data Privacy Framework invalidated (Schrems III), making current data transfers illegal	Legal / Regulatory	3/5	4/5	major	Legal exposure
R-04	Stripe parent company subject to US sanctions or regulatory action affecting EU payment processing	Operational / Geopolitical	1/5	5/5	major	Inferred
R-05	DORA ICT third-party risk requirements not met for fintech clients who require SOC 2 or NIS2 compliance from suppliers	Regulatory / Commercial	3/5	3/5	moderate	Legal exposure
R-06	Shadow IT: unaudited browser extensions and OAuth grants expose data to unknown third parties	Security / Shadow IT	3/5	3/5	moderate	Observed
R-07	Customer PII stored in US-hosted services (Intercom, Slack) without adequate legal basis for transfer	Legal / GDPR	4/5	3/5	major	Observed

L = Likelihood (1–5). I = Impact (1–5). Ev. = Evidence basis (Obs. = Observed, Legal = Legal exposure, Inf. = Inferred).

4.3 Risk Heatmap



Two risks fall in the critical zone (R1: CLOUD Act exposure, R2: Google single-point-of-failure). The concentration in the high-likelihood / high-impact quadrant reflects the near-total US dependency.

4.4 Jurisdictional Exposure Detail

United States: CLOUD Act (2018)

The CLOUD Act[7] allows US law enforcement to compel US-headquartered technology companies to provide data regardless of storage location. Under most circumstances, no prior notification to the data subject or foreign government is required, though the act provides for a comity analysis in some cases.

Potential implications for Veldstra Finance:

- All 14 US-headquartered services may be subject to such requests, including those with EU data residency
- EU data residency alone does not prevent CLOUD Act requests; the legal obligation follows the corporate parent
- The EU-US Data Privacy Framework (2023)[8] faces ongoing legal challenge and could be invalidated (as Safe Harbor and Privacy Shield were)

[7] Clarifying Lawful Overseas Use of Data Act, 18 U.S.C. § 2713 (2018). Full text: congress.gov/bill/115th-congress/house-bill/4943.

[8] European Commission Implementing Decision (EU) 2023/1795 of 10 July 2023.

FISA Section 702

Permits warrantless surveillance of non-US persons' communications on US electronic communication services.[9] This provision may apply to Veldstra Finance employees, depending on how the services in use are classified and whether communications are targeted.

4.5 Regulatory Compliance Mapping

Requirement	Current state	Gap	Action
GDPR Art. 28: Processor agreements	DPAs in place for major vendors	Not reviewed for CLOUD Act conflict	Review all DPAs with counsel
GDPR Ch. V: International transfers	Relying on EU-US DPF + SCCs	No contingency if DPF invalidated	Migration plan is the contingency
GDPR Art. 32: Security of processing	E2E encryption on 1Password only	Most services: transport encryption only	Evaluate E2E alternatives
DORA Art. 28: ICT third-party risk	No formal register	No exit strategies documented	This audit serves as the starting register

DORA applicability depends on Veldstra Finance's classification as a financial entity or ICT third-party provider. Included as a reference framework given the fintech sector context.

[9] 50 U.S.C. § 1881a. Reauthorised April 2024 through 2026.

Replacement Analysis

For: CTO, IT, procurement

Key question: What are the alternatives, and how do they compare?

5.1 Replacement Shortlist

Current	Recommendation	Sov.	Fit	Effort	Key gaps
Google Workspace	Proton for Business + Nextcloud	3/4	Adequ	medium	Calendar sharing less polished (CalDAV). Mobile apps functional but not as refined. Document co-editing via Collabora has slight latency.
Slack	Element (Matrix protocol)	3/4	Adequ	easy	Thread UX less mature. App ecosystem smaller. Used by French and German governments. E2E encrypted.
GitHub	GitLab (EU SaaS or self-managed)	3/4	High	medium	Repo migration straightforward. CI/CD pipelines need rewriting from GitHub Actions to GitLab CI.
Notion	Outline	4/4	Adequ	easy	No database views like Notion. Markdown-native wiki/knowledge base.
Figma	Penpot	4/4	Gaps	easy	SVG-native. Lacks advanced prototyping. Figma file import improving.
Linear	Plane	4/4	Adequ	easy	Clean UI. Cycle planning, issue tracking.
Vercel	Scaleway Serverless + CDN	4/4	Adequ	easy	No built-in preview deployments like Vercel. Minor pipeline changes.
Stripe	Mollie	4/4	Gaps	hard	No Stripe Connect equivalent for marketplace features. Significant API rework required.
AWS (S3 + CloudFront)	Scaleway Object Storage + CDN	4/4	High	medium	S3-compatible API. Terraform provider available.
Intercom	Crisp	4/4	Adequ	easy	Lacks some Intercom automation features. Live chat, help centre, chatbot all present.
HubSpot	Brevo (formerly Sendinblue)	4/4	Adequ	medium	CRM less mature than HubSpot but adequate for team of 2. Good email campaigns.

Current	Recommendation	Sov.	Fit	Effort	Key gaps
1Password	Proton Pass (Business)	3/4	High	easy	E2E encrypted. 1Password export supported. Newer product, fewer browser integrations.
Zoom	Jitsi Meet	4/4	Adequ	easy	No recording or breakout rooms. No account needed for guests. Score assumes EU-hosted deployment.
Sentry	GlitchTip	4/4	Gaps	easy	Fewer features but covers core error tracking. Sentry SDK-compatible.
PostHog	Plausible Analytics	4/4	Poor	easy	Lacks product analytics (funnels, session replay, feature flags). Web analytics only.

Sovereignty: 0/4 *None* · 1/4 *Low* · 2/4 *Moderate* · 3/4 *High* · 4/4 *Full EU* · *Replaceability:* 🟢 *Easy* · 🟡 *Medium* · 🟠 *Hard* · 🔴 *DNT* · *See §2.3.*

Fit: High = covers core workflows. Adequate = workable with minor adjustments. Gaps = significant missing features. Poor = not viable.
Cost details: licensing and hosting cost comparison in Section 6.5.
Sovereignty for self-hosted tools: scores assume deployment on EU infrastructure (Scaleway). Using a vendor-hosted or public free instance may lower the effective sovereignty score.

5.2 Feature Parity: Google Workspace to Proton + Nextcloud

This is the only migration where the decision is genuinely uncertain. Zoom to Jitsi is obvious; this one has real gaps that need visibility.

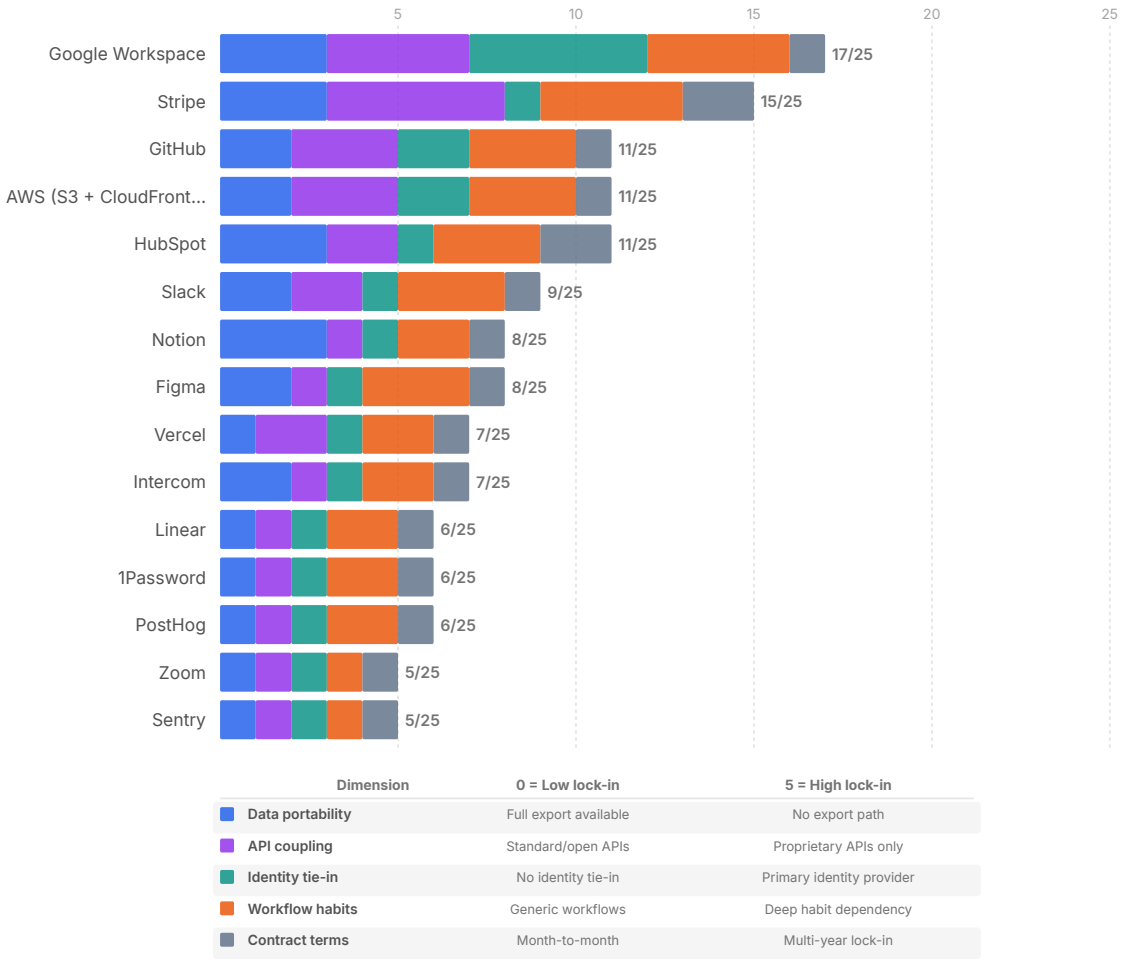
Feature	Google	Proton + Nextcloud	Notes
Email	●	●	Proton Mail fully featured
Calendar	●	◐	CalDAV; sharing UX less polished
File storage	●	●	Nextcloud with EU managed hosting
Document editing	●	◐	Collabora Online; slight co-editing latency
Spreadsheets	●	◐	Collabora; formula compatibility adequate
Video calls	●	●	Jitsi Meet integration
Mobile apps	●	◐	Functional but less polished

Feature	Google	Proton + Nextcloud	Notes
Admin console	●	◐	Two separate admin panels
SSO/SAML	●	●	Both support SAML/OIDC
E2E encryption	○	●	Proton E2E encrypted by default

● = Full · ◐ = Partial · ○ = Not available

Bottom line: Adequate for core workflows. The main friction points are calendar sharing and document co-editing, both workable for an 8-person team but noticeably less polished than Google.

5.3 Lock-in Severity



Stripe has the highest lock-in, driven by deep API integration and workflow coupling. Google Workspace scores high on identity lock-in (SSO for 6 services). Most other services have low lock-in.

Roadmap & Action Plan

For: CEO, CTO, operations

Key question: What do we do, in what order, and what does it cost?

Migration planning is part of this audit. Migration execution (hands-on cutover) is a separate engagement.

6.1 Prerequisites

Before any migration begins, the following must be true:

- **Decision authority:** CTO has confirmed mandate to proceed with Phase 0 quick wins
- **Data export verified:** Google Takeout tested for email, Drive, Calendar; export is complete and usable
- **Alternative accounts provisioned:** Proton, Nextcloud, Crisp trial accounts active
- **DNS control confirmed:** Domain registrar access available for MX record changes
- **Team availability:** At least 1 person available for 2–3 hours/week to support migration tasks

For an 8-person team, these prerequisites can typically be met in a single afternoon.

6.2 Sequenced Recommendations

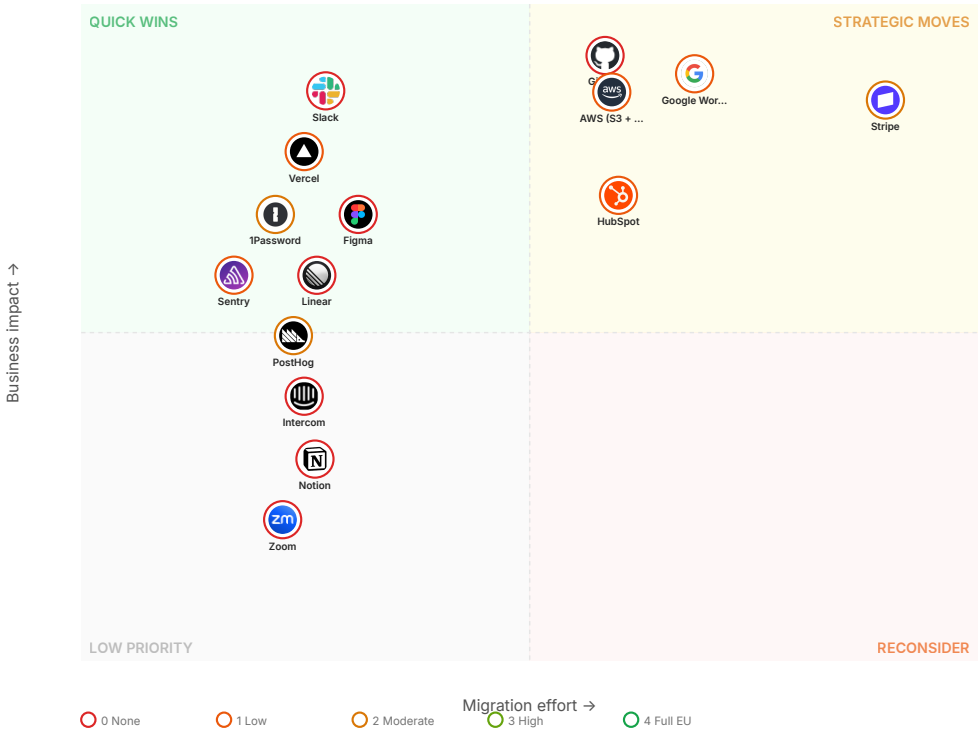
Phase 0: Quick Wins (Days) Revoke shadow IT OAuth grants. Document current SSO dependencies. Move services with drop-in EU alternatives: Intercom → Crisp, Zoom → Jitsi, 1Password → Proton Pass. These require minimal planning and can run in parallel.

Phase 1: Reduce Exposure (Weeks 1–3) Deploy standalone EU identity provider (Authentik) and pilot with 2 non-critical services. This begins the decoupling of identity from Google. Trial Proton Mail with 2 pilot users. Deploy managed Nextcloud. Migrate Sentry to GlitchTip, Linear to Plane, Notion to Outline.

Phase 2: Deepen Independence (Weeks 3–8) Full Google Workspace → Proton + Nextcloud migration. GitHub → GitLab (CI/CD pipeline rewrite). AWS → Scaleway. HubSpot → Brevo. These have dependencies on each other and need sequencing.

Phase 3: Strategic Completion (Month 3+) Complete identity cutover: migrate all remaining services from Google SSO to standalone EU IdP. Evaluate Stripe to Mollie migration path. These are long-horizon items; identity cutover depends on Phases 1–2 completing, and Stripe depends on feature gap analysis.

6.3 Priority Matrix



Quick wins (low effort, high impact) are in the top-left: Intercom, Zoom, shadow IT revocation. Stripe is bottom-right: highest effort, highest strategic importance, longest timeline.

6.4 Action Items

ID	Action	Phase	Owner	Effort
A-01	Audit Google Workspace OAuth grants and revoke all unrecognised third-party access	0: Quick wins	CTO	2 hours
A-02	Document current SSO/OAuth dependencies: which services authenticate through Google Workspace	0: Quick wins	CTO	2 hours
A-03	Replace low-risk US tools with EU drop-in alternatives (Zoom to Jitsi, Intercom to Crisp, 1Password to Proton Pass)	0: Quick wins	CTO	3 days
A-06	Deploy standalone EU identity provider (Authentik) and pilot with 2 non-critical apps	1: Reduce exposure	CTO	1 week
A-07	Trial Proton for Business with 2 pilot users (email + calendar) and deploy managed Nextcloud	1: Reduce exposure	CTO	1 week
A-09	Migrate collaboration stack to EU self-hosted alternatives (Sentry to GlitchTip, Linear to Plane, Notion to Outline)	1: Reduce exposure	CTO	1 week
A-12	Full Google Workspace to Proton + Nextcloud migration for all users (email, calendar, drive)	2: Deepen independence	CTO	2 weeks
A-13	Migrate infrastructure stack: GitHub to GitLab, AWS to Scaleway, HubSpot to Brevo	2: Deepen independence	CTO	3 weeks
A-16	Complete identity cutover: migrate all remaining services from Google SSO to standalone EU IdP	3: Strategic completion	CTO	2 weeks
A-17	Evaluate Stripe to Mollie migration path; document API differences and build migration plan	3: Strategic completion	CTO	2 weeks (eval)

10 primary actions shown. Detailed sub-actions (per-service migration steps, pilot configurations) provided as CSV alongside this report.

6.5 Cost Comparison

Category	Current	Licensing	Hosting	Net Δ
Email, Calendar & Docs	€1,152/yr	€1,248/yr	€180/yr	+€276
Messaging (Slack → Element)	€816	€480	€0	−€336
Documentation (Notion → Outline)	€768	€0	€60/yr	−€708
Source Code (GitHub → GitLab)	€456	€432	€0	−€24
Hosting (Vercel → Scaleway)	€240	€180	incl.	−€60
Cloud Infra (AWS → Scaleway)	€3,600	€2,880	incl.	−€720
Support (Intercom → Crisp)	€1,560	€600	€0	−€960
CRM (HubSpot → Brevo)	€1,200	€600	€0	−€600
Password (1Password → Proton Pass)	€384	€384	€0	€0
Video (Zoom → Jitsi)	€168	€0	€0	−€168
Error Mon. (Sentry → GlitchTip)	€312	€0	€60/yr	−€252
Project (Linear → Plane)	€576	€0	incl.	−€576
Design (Figma → Penpot)	€360	€0	€0	−€360
Analytics (PostHog)	€0	€0	€0	€0
Payments (Stripe)	variable	eval.	n/a	TBD
Total (excl. Stripe)	**€11,592**	**€6,804**	**€300**	**−€3,888/yr**

Hosting: self-hosted services (Outline, Plane, GlitchTip) estimated at shared Scaleway VPS €25/mo total. Managed Nextcloud €15/mo.
Operations: self-hosted tools require 3–4 hrs/month maintenance (updates, monitoring). For an 8-person team with a technical CTO, this is manageable. For non-technical teams, managed EU SaaS alternatives exist at higher cost.
Migration execution costs (labour, consulting) not included; scoped separately.

6.6 Migration Risks

For an 8-person team, migration risks are manageable. The key risk per phase:

- **Phase 0:** Crisp lacks a specific Intercom automation → 2-day pilot first; revert if needed
- **Phase 1:** Proton Mail deliverability issues → keep Google Workspace active in parallel during 1-week pilot. Authentik IdP misconfiguration → pilot with non-critical apps only.
- **Phase 2:** GitLab CI pipeline failures → dual-push to both GitHub and GitLab during transition
- **Phase 3:** Identity cutover breaks service access → staged per-service cutover with rollback plan. Mollie API gaps → maintain Stripe as primary; Mollie as secondary evaluation path.

Appendices

Appendix A: Full Dependency Inventory

Complete inventory with all fields provided as CSV alongside this report (`veldstra-dependency-inventory.csv`).

CSV fields: Service, Vendor, HQ, Data Processing Locations, Contract Type, Renewal Date, Auth Method, Data Types Processed, Est. Data Volume, Integration Points, Admin Access Holders, Sovereignty Score, Replaceability, Evidence Basis.

Preview (3 rows, redacted):

Service	Vendor	HQ	Data Loc.	Contract	Renewal	Auth	Data Types
Google Workspace	Google LLC	US	EU (region)	Monthly	2026-07-01	Primary IdP	PII, financial, IP
Stripe	Stripe Inc.	US	EU (IE)	Rolling	n/a	API keys	PII, financial
Intercom	Intercom Inc.	US	US + AU	Monthly	2026-03-01	Google SSO	PII, operational

Full 15-row CSV with all fields accompanies this PDF.

Appendix B: Sovereignty Scoring Detail

Sovereignty: 0/4 *None* · 1/4 *Low* · 2/4 *Moderate* · 3/4 *High* · 4/4 *Full EU* · *Replaceability:* 🟢 *Easy* · 🟡 *Medium* · 🟠 *Hard* · 🔴 *DNT* · *See §2.3.*

Service	Strategic	Legal	Operational	Data	Supply Ch.	Technology
Google Workspace	0	1	2	2	0	1
Slack	0	0	0	0	0	0
GitHub	0	0	1	0	0	1
Notion	0	0	0	0	0	0
Figma	0	0	0	0	0	0
Linear	0	0	0	0	0	0
Vercel	0	0	1	1	0	1
Stripe	0	2	2	2	1	1
AWS	0	1	2	2	0	1
Intercom	0	0	0	0	0	0
HubSpot	0	1	1	2	0	1
1Password	1	2	2	3	1	2
Zoom	0	0	0	0	0	0
Sentry	0	0	1	1	0	2
PostHog	0	1	2	2	0	3

Dimensions: Strategic = EU ownership/governance. Legal = jurisdiction and extraterritorial exposure. Operational = control over service continuity. Data = residency, encryption, access controls. Supply Chain = upstream dependencies. Technology = open standards, portability.

Appendix C: Integration Map

Key integration relationships (detailed in Section 3.2 graph):

- **OAuth/SSO:** Google Workspace → Slack, Figma, Linear, Intercom, Notion, Sentry
- **Webhook:** GitHub → Slack, Linear → Slack, Sentry → Slack
- **CI/CD trigger:** GitHub → Vercel
- **API:** Stripe ↔ AWS, Sentry → GitHub

Appendix D: Regulatory Reference

US CLOUD Act (2018)[10]: Allows US authorities to compel US companies to provide data regardless of storage location. Notification requirements vary; the act includes a comity analysis provision for qualifying foreign government objections.

FISA Section 702[11]: Permits surveillance of non-US persons' communications on US electronic communication services. Scope and application depend on how services are classified and whether communications are targeted.

EU-US Data Privacy Framework (2023)[12]: Adequacy decision adopted July 2023. Legal challenge pending (NOYB, potential "Schrems III"). Previous frameworks (Safe Harbor, Privacy Shield) were invalidated by the CJEU.

GDPR Chapter V[13]: International transfers require adequacy decision, SCCs/BCRs, or derogations. Transfer Impact Assessments required when relying on SCCs.

DORA (2022/2554)[14]: Exit strategies required for critical ICT services (Article 28). Applies to financial entities and their ICT third-party providers. Applicability to Veldstra Finance depends on entity classification.

NIS2 (2022/2555)[15]: Supply chain security and incident reporting for essential/important entities. Applicability depends on sector and entity size thresholds.

Appendix E: Glossary

CLOUD Act	US law allowing data access regardless of storage location
Control plane	Service that others depend on for authentication or operation
Data residency	Physical location where data is stored
DPA	Data Processing Agreement (GDPR requirement)

[10] 18 U.S.C. § 2713.
[11] 50 U.S.C. § 1881a. Reauthorised through 2026.
[12] European Commission Implementing Decision (EU) 2023/1795.
[13] Regulation (EU) 2016/679, Articles 44–50.
[14] Regulation (EU) 2022/2554, Digital Operational Resilience Act.
[15] Directive (EU) 2022/2555, Network and Information Security Directive.

DPF	EU-US Data Privacy Framework (2023 adequacy decision)
E2E encryption	End-to-end encryption; only sender and recipient can read data
FISA 702	US foreign intelligence surveillance provision
IdP	Identity Provider (manages user authentication)
Lock-in	Difficulty of switching away from a vendor
OAuth	Open standard for access delegation
SCC	Standard Contractual Clauses (EU transfer mechanism)
SEAL	Sovereignty Effectiveness Assurance Level (EU framework, 0–4)
Shadow IT	Technology used without IT department approval
SSO	Single Sign-On (one login for multiple services)

Appendix F: Interview Notes

Interview: CTO, 2026-02-10, 60 minutes (video call)

Key points:
- Stack assembled opportunistically 2022–2023 with no sovereignty considerations
- Google Workspace chosen because “everyone uses it”; no alternatives evaluated
- Stripe chosen for developer experience; team acknowledges deep lock-in
- Growing concern from prospective enterprise clients about data sovereignty
- No budget pressure to change; motivation is regulatory and commercial risk
- CTO prefers open-source where viable
- No formal IT policy or vendor evaluation process

End of report.