Geopolitical uncertainty and the cloud

Christian Thindberg
Statistics Norway
christian.thindberg@ssb.no

Keywords: cloud-native, open source, data platform, data states, geopolitical risk

1. Introduction

National statistical institutes (NSIs) operate under triple pressure. Users expect faster, more granular and methodologically transparent statistics. Analytical tools in machine learning need scalable infrastructure that is awkward to provision on-premises. The regulatory and geopolitical landscape has also shifted: EU–US transfer rules have been rewritten twice in a decade, and US executive action now reaches deeper into US providers serving European customers (Politico, 2025; Forbes, 2025). Commercial cloud answers the first two pressures with scale, elasticity and managed services, while introducing the new dependencies and strategic uncertainties the third pressure foregrounds. For an NSI these tensions interact acutely. Official statistics depend on long-term institutional trust, the protection of confidential microdata and uninterrupted production. The cost of a wrong platform choice is not bounded by a procurement cycle.

Statistics Norway (SSB) adopted a cloud-first strategy in 2018 and has migrated substantial parts of its data, services and production to Google Cloud Platform (GCP). The strategy rests on three principles: comprehensive cloud migration; open standards, open-source components and cloud-native architecture such as Kubernetes to limit lock-in; and metadata-driven data management with strong security to keep production stable and transparent across platforms. Recent events, examined in Section 4, have placed this strategy under scrutiny and sharpened the European debate about digital sovereignty.

The paper introduces a six-dimension framework for evaluating cloud and on-premises options under geopolitical uncertainty. It draws on US sanctions practice, EU–US transfer law and Norwegian guidance from NSM (Norwegian National Security Authority) and DFØ (Norwegian Agency for Public and Financial Management). Applied to SSB, with comparison to a fully European cloud, it finds that several risks commonly attributed to commercial cloud are overstated for an NSI workload. A legacy on-premises environment, by contrast, carries higher exposure on security, exit cost and regulatory compliance. A cloud strategy based on open standards therefore strengthens resilience, provided the architecture preserves the option to change provider. The paper closes with lessons for other NSIs.

2. A framework for cloud risk under geopolitical uncertainty

Public-sector risk assessments of cloud commonly focus on the legal reach of US intelligence. This produces two errors: comparison against an idealized on-premises baseline that ignores actual legacy systems, and omission of longer-horizon risks, above all the cost of changing platforms. NSM concludes that cloud benefits outweigh drawbacks for most organisations given sound prior assessment, and that most cloud-related incidents arise from customer-side misconfiguration rather than provider failure (NSM, 2020). On the other hand, NSM also warns about national-level dependency on a few foreign providers (NSM, 2026). Procurement guidance adds that a residual risk of foreign-intelligence access does not by itself disqualify a cloud option. Its magnitude must be weighed against the alternatives (DFØ, 2022).

To facilitate a holistic risk approach, this paper applies a six-dimension framework: intelligence activity and confidentiality; kill switch, the forced suspension of services; exit cost and vendor lock-in; price and contract risk; privacy and regulatory transfer; and political control and continuity. Each is a distinct mechanism by which platform choice affects resilience, cost or compliance over a long horizon. Section 4 takes them up in turn.

3. SSB's cloud-first strategy and the Dapla platform

Statistics Norway adopted a formal cloud-first strategy in 2018, migrating much of a legacy stack based on Oracle, SAS, Fame and Microsoft to a cloud-native[1] environment on GCP. The migration redesigns statistical production around modular open-source components, declarative infrastructure and explicit data-state management.

3.1 Three principles

The first principle is comprehensive cloud migration, for shorter development cycles and analytical capabilities impractical at SSB's scale on-premises. The second is open standards and cloud-native architecture. Workloads run on Kubernetes through the NAIS platform (see nais.io), with the Onyxia data-science portal from INSEE (Comte et al., 2023) and an open-source analytical stack. Platform-specific proprietary services are

[1] Cloud native is an architectural pattern designed to benefit from modern IT-infrastructures characterized by open source, containerization and infrastructure as code. It give organizations room for maneuvre as own developed systems are no longer tied to particular operating systems or physical infrastructure.

avoided, which is what makes provider substitution feasible. The third is metadata-driven data management around the five data states defined in SSB's note 2024/44 (Statistics Norway, 2024).

3.2 The Dapla platform and implemented security measures

All production data are stored and processed in europe-north1 (Finland), meeting the GDPR requirement for storage at rest within the EEA. Data are encrypted at rest with AES-256 using Google-managed keys, identifiers are pseudonymized, and source-data access is just-in-time with full audit logging. VPC Service Controls confine Dapla to a defined perimeter, and contractual safeguards include Standard Contractual Clauses and the OCRE framework (GÉANT, 2025).

3.3 The cryptographic gap and SSB's risk-based position

Implemented measures protect against external attackers and limit insider access. Since encryption keys are administered by Google, a US CLOUD Act order could compel disclosure, but any order would be limited to defined persons or entities, not the dataset as a whole. SSB has not adopted customer-managed keys or a multi-cloud architecture with a qualified European provider for the most sensitive data states. The decision is risk-based. The CLOUD Act and FISA 702 require a concrete national-security or terrorism nexus, and the probability that SSB's statistical microdata meets it is very small. SSB will reassess if the threat picture, the law or platform use changes materially.

4. Applying the framework

Each dimension is assessed against two alternatives. The first is a fully European cloud: a European-owned provider running open-source or European software, with no US-licensed software in the critical parts. The second is on-premises operation augmented for modern demands. Assessments are qualitative (Low, Medium, High), summarised in Table 1.

Table 1. Comparative threat matrix

Dimension	Cloud	European cloud	On-premises
1. Intelligence activity / confidentiality	Low	Medium	High
2. Kill switch	Low	Low	Low
3. Exit cost / vendor lock-in	Medium	Medium	High
4. Price and contract risk	High	High	High
5. Privacy and regulatory transfer	Medium	Low	Low
6. Political control and continuity	Medium	Medium	Medium

4.1 Dimension 1: Intelligence activity and confidentiality

Open assessments place Russia, China and Iran at the centre of the confidentiality threat (NSM, 2026; PST, 2026; Etterretningstjenesten, 2026). The hyperscale providers offer security and incident response at a scale on-premises deployments do not match. As described in section 3.3. the Cloud Act risk is very small for an NSI. The on-premises alternative on the other hand carries a documented risk. Over three years of penetration testing, NSM identifies technical debt and unsupported legacy systems among the most persistent vulnerabilities in Norwegian IT (NSM, 2023). Its own recommendation is modernization toward professionally operated cloud-native platforms. A European provider escapes US jurisdiction but trails the hyperscalers on technical security. Risk: Low (cloud), Medium (European cloud), High (on-premises).

4.2 Dimension 2: Kill switch

Forced service disruption has moved from theoretical concern to documented case. Two events show distinct mechanisms.

Case 1: US sanctions and the ICC. Executive Order 14203 (6 February 2025) sanctioned the International Criminal Court and named officials. Within weeks Microsoft disconnected the Chief Prosecutor's ICC email account, and the Court moved to Proton Mail and openDesk, a German open-source suite (Irish Legal News, 2025). Read as proof that the US could disable cloud across Europe, the case overreaches: the order targeted named individuals under existing sanctions authority[2], and the service was a personal account. The accurate reading is narrower, that a targeted sanction propagates compliance obligations onto US providers that reach the European customer.

Case 2: US export controls and AI models. On 12 June 2026 a US Commerce Department directive ordered a US provider to suspend access to two AI models for any foreign national. Unable to identify nationality in real time, the provider disabled both models worldwide (Anthropic, 2026). The directive overrode the AI-authorisation whitelist on which Norway appears. It showed that access to a US-operated service can be

[2]The US sanctions framework administered by OFAC distinguishes between comprehensive country-based programmes and list-based designations under the Specially Designated Nationals (SDN) and related lists. Compliance obligations under EO 14203 attach to listed individuals, not to the institution or host country as such (Congressional Research Service, 2025).

revoked for a whole foreign user base by order, regardless of where data reside. This is a service-availability mechanism, distinct from the ICC's data-access mechanism.

Neither case generalises to SSB. Sanctions on named individuals do not shut down cloud services across Europe, and export controls on specific AI models do not extend to cloud infrastructure. Substituting one AI model for another is easy; re-platforming production is not. The open-standards architecture keeps switching cost within bounds (Dimension 3). Risk: Low (cloud), Low (European cloud), Low (on-premises)[3].

4.3 Dimension 3: Exit cost and vendor lock-in

The legacy stack (SAS, Oracle, Fame) carries substantial exit cost: data and logic entangled with products, a narrow skills market, and migrations that often fail to retire the original system (Jørgensen, 2026). Dapla inverts this through Kubernetes, open columnar storage formats such as Parquet, analytical code in open languages and a cloud-agnostic portal. Risk: Medium (cloud), Medium (European cloud), High (on-premises).

4.4 Dimension 4: Price and contract risk

Cloud markets show episodic price restructuring; on-premises carries parallel exposure through rising proprietary licence fees, hardware refresh cycles and operating costs. SSB's portability preserves bargaining power by making substitution credible. Still: rising prices are expected for all operating models. Risk: High (cloud), High (European cloud), High (on-premises).

4.5 Dimension 5: Privacy and regulatory transfer

The Court of Justice has twice struck down the EU–US transfer arrangement: Safe Harbor in *Schrems I* (2015) and Privacy Shield in *Schrems II* (2020) (Court of Justice of the European Union, 2020). Each time a replacement followed, most recently the EU–US Data Privacy Framework (European Commission, 2023). There is risk in that the framework may be challenged again in the future, or that EU revokes the adequacy decision regarding the US. Under such circumstances SSB must do a new risk assessment and consider appropriate action. As the consequences of EU and US not

[3] Most software today has a built in "kill switch" - it requires a valid licence key to run. Hence, the risk of forced service disruption also applies to on-premises operations.

resolving this issue are very high on both sides, probability is low. Still, a consequence could be that SSB would have to switch provider. On-premises and European cloud would remove the risk completely, at the cost of higher exposure on other dimensions. Risk: Medium (cloud), Low (European cloud), Low (on-premises).

4.6 Dimension 6: Political control and continuity

US-software dependence predates the cloud and is widespread across the public sector regardless of platform; on-premises does not escape it. The relevant question is whether the architecture preserves the option to change direction. Dapla meets this through open standards and cloud native.

A European region of a US hyperscaler, or a European provider running US-licensed software, is still exposed to EU-US political turmoil. As an example, the company S3NS runs Google Cloud under French control with SecNumCloud qualification (Thales, 2025). This shields data against the CLOUD Act, but its US-licensed software stays exposed to "kill switch", trade barriers and other issues that may occur due to EU-US tensions.

There is political pressure within Europe towards more European solutions, and so preserving room for maneuver is important. This applies equally to all alternatives.

Risk: Medium (cloud), Medium (European cloud), Medium (on-premises).

5. Conclusion

For organizations that need to modernize the cloud hyperscalers offer unprecedented scale, flexibility and technology, making them attractive partners for organizations that need to modernize. Also, across the six dimensions SSBs cloud-first strategy is at least as resilient as the European cloud or legacy stack on all but privacy and regulatory transfer, and clearly stronger on intelligence-grade security and exit cost. Three caveats temper this. The cryptographic gap of Section 3.3 needs reassessment if the threshold shifts; at a national level the concentration risk is real (NSM, 2026); and a reader expecting rapid deterioration of transatlantic relations would weigh Dimensions 2, 5 and 6 more heavily. The framework makes these priors explicit on individually assessable dimensions, and we hope this approach may be useful for other members of the statistical community.

Appendix: List of references

Anthropic (2026). Statement on the US government directive to suspend access to Fable 5 and Mythos 5. 12 June 2026.

Comte, F., Degorre, A., & Lesur, R. (2023). Onyxia: An open source cloud native data science platform. International Statistical Institute World Statistics Congress 2023, Ottawa.

Congressional Research Service (2025). U.S. Sanctions: Overview for the 119th Congress. CRS Report IF12390. Library of Congress, Washington, DC.

Court of Justice of the European Union (2020). Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II), Case C-311/18.

DFØ – Direktoratet for forvaltning og økonomistyring (2022). Markedsplassen for skytjenester: Hjelp til å vurdere personvernrisikoen for innhenting til etterretningsformål ved bruk av skytjenester. Anskaffelser.no.

Etterretningstjenesten (2026). Fokus 2026. Norwegian Intelligence Service, 6 February 2026.

European Commission (2023). Commission Implementing Decision (EU) 2023/1795 on the adequate level of protection of personal data under the EU-US Data Privacy Framework. Brussels.

Executive Order 14203 (2025). Imposing Sanctions on the International Criminal Court. The White House, 6 February 2025. Federal Register.

Forbes (2025). Microsoft Can’t Keep EU Data Safe From US Authorities. By E. Woollacott. 22 July 2025.

GÉANT (2025). OCRE 2024 Framework: Open Clouds for Research Environments. clouds.geant.org.

Irish Legal News (2025). ICC to ditch Microsoft following US sanctions. 31 October 2025.

Jørgensen, M. (2026). Å tenke på slutten i starten – om avvikling og Helseplattformen. Computerworld, 8 May 2026.

NAIS. The NAIS application platform. Norwegian Labour and Welfare Administration. nais.io.

NSM – Nasjonal sikkerhetsmyndighet (2020). Helhetlig digitalt risikobilde 2020. Oslo.

NSM – Nasjonal sikkerhetsmyndighet (2023). Ti sårbarheter i norske IKT-systemer: Erfaringer fra NSMs inntrengingstester. Oslo.

NSM – Nasjonal sikkerhetsmyndighet (2026). Risiko 2026. Oslo.

Politico (2025). Microsoft would push back against Trump order to suspend European cloud operations. 30 April 2025.

PST (2026). Nasjonal trusselvurdering 2026. Politiets sikkerhetstjeneste, 6 February 2026.

Statistics Norway (2024). Notat 2024/44: Datatilstander i SSB. Oslo, 28 October 2024.

Thales (2025). S3NS receives SecNumCloud qualification: a turning point for trusted cloud solutions. Thales Group, 19 December 2025.