Varnish

RESEARCH REPORT

Europe's Public Sector and News Websites Run on a US Edge

How 1,122 government bodies and media organisations in 30 European countries deliver their websites, and what it means for cyber resilience, NIS2, GDPR, and the US CLOUD Act.

Summary

The overlooked layer of digital sovereignty

Europe is rewriting the rules on digital dependency, from NIS2 and the Cyber Resilience Act to proposed sovereignty tests for public-sector cloud. Despite this, one layer that every citizen and reader passes through has stayed largely out of view: the network edge.

Digital sovereignty has moved from policy papers into procurement. In April 2026, the European Commission awarded €180 million in sovereign cloud contracts, then proposed the Cloud and AI Development Act, which would make sovereignty a formal test for public buyers. Meanwhile, the legal basis for transatlantic data flows has grown less certain. Since 2018 the US CLOUD Act has required US providers to hand over data in their control wherever it is stored; FISA Section 702 lapsed in June; and the EU-US Data Privacy Framework faces a further court challenge. US sanctions against international officials and service providers have also shown that access to everyday digital services, from email and productivity software to hosting infrastructure, is increasingly subject to geopolitical crosswinds.

The CDN Is an underappreciated risk

So far, the sovereignty debate has focused on data at rest: where databases and documents are stored, and which cloud region hosts them. Far less attention has been paid to data in transit. Before a request reaches those data stores, it usually passes through a content delivery network (CDN), the layer known as the network edge. A CDN answers visitors on a website's behalf and keeps logs of every request. That makes it a single point of failure: when one provider has an outage, every site behind it goes offline. It is also a jurisdictional exposure, because the market is dominated by a handful of US companies that answer to US law wherever their servers sit. Yet the edge is rarely managed as a regulated supplier: it is often chosen by a web agency, bought as a commodity, and absent from risk registers.

We found no public, Europe-wide picture of who operates the edge for the institutions that citizens depend on. The answers bear on NIS2 and GDPR compliance, on readiness for the sovereignty assessments now proposed, and on whether crisis channels stay reachable when they are needed most. They describe a continent that has largely made this choice by default rather than by design.

The Study

1,122
government and media organisations

30
countries: EU 27, UK, Norway, Iceland

4,705
hostnames traced to provider and jurisdiction

Key findings 3
Finding 1: Continuity 4
Finding 2: Jurisdiction 5
Finding 3: Exposure 6
Compliance map 7
Recommendations 8
A practical response and method 9
Sources 10

Key findings

Results in brief

More than half of Europe's public sector and news websites (511 of 915, or 56%) are delivered through a US-headquartered CDN. Most of the rest have no CDN in front of them at all. European CDNs serve just 1.2%.

We scanned 1,122 government bodies and news organisations in 30 European countries on 12 and 13 October 2026. Figures count each unique website once unless stated.

Metric	Result
Sites whose edge is a US-headquartered provider	**56%** (511 of 915)
Sites behind the four largest US providers	**49%** (445)
Sites behind the single largest provider, Cloudflare	**28%** (254)
Sites that use a CDN and chose a US one	**96%** (482 of 502)
Sites with no CDN at the edge	**45%** (413), including **59%** of government sites
Sites behind European-headquartered CDNs	**1.2%** (11)
News and broadcast sites vs government sites on a US edge	**77%** (292 of 377) vs **41%** (219 of 538)
Organisations running more than one CDN that use only US providers	**85%** (94 of 110)

Three risks

Concentration

Four US providers front almost half of all sites; one provider outage can take several governments' websites down at once.

Jurisdiction

Most protected sites sit with providers subject to US law, including the CLOUD Act, wherever their servers are located.

Exposure

Nearly half of all sites show no CDN protection against traffic surges or DDoS attacks.

Finding 1

Business continuity rests on a handful of providers

49% Four US providers front 445 of 915 sites, and Cloudflare alone fronts 254 (28%). When one of them fails, sites in many countries fail together.

Governments often place every ministry behind one shared platform and one CDN. That simplifies operations but presents a single point of failure for an entire government's web presence.

Government platform	Country	Bodies	Edge CDN
Government Digital Service	UK	28	Fastly (27), CloudFront (1)
MITA	Malta	26	Cloudflare (25), self-hosted (1)
Deputy Ministry of Research, Innovation and Digital Policy	Cyprus	20	Azure Front Door
DSS	Norway	19	Cloudflare (18), Azure Front Door (1)
Gov.ie / OGCIO	Ireland	18	Amazon CloudFront
Office of the Government	Lithuania	15	Cloudflare
Rijksoverheid platform, DPC	Netherlands	14	Akamai
Valitsusportaal, RMIT	Estonia	14	Cloudflare
Joint government web service, VNK	Finland	14	Cloudflare

Why it matters

The failures that take sites offline are often configuration errors inside the provider.

Date	Provider	What happened
20 Feb 2026	Cloudflare	A faulty internal clean-up task withdrew about 1,100 customer IP prefixes from the internet, leaving affected services unreachable for up to six hours.
18 Nov 2025	Cloudflare	A malformed Bot Management file caused global HTTP errors from 11:20 to 17:06 UTC; government and news sites in several countries were affected.
19–20 Oct 2025	AWS	An empty DNS record for DynamoDB in us-east-1 cascaded across dependent services for about 14 hours.

Only 110 of 1,122 organisations (10%) showed more than one CDN anywhere across their web and API hostnames, and 94 of those used US providers only. For the rest, we saw no sign of a second delivery path if the first one fails, and where a second path does exist, it rarely sits under a different jurisdiction.

The other side

Shared platforms are not only a US-provider pattern. National self-hosted platforms each serve more than 20 bodies from one infrastructure. Consolidation brings real gains in security, patching, and cost; the risk lies in having no tested alternative when that single path fails.

Finding 2

Jurisdiction risk from the CLOUD Act and US sanctions

For 511 of Europe's public-interest websites, the company that answers every visitor request is bound by US law. Hosting in an EU data centre does not change that.

A CDN sits in front of a website and handles visitor requests on its behalf. In doing so it generates metadata and logs: visitor IP addresses, resources requested, timestamps, and device details. Together, those records show who accessed which public service, and when. Under the CLOUD Act (18 U.S.C. § 2713), in force since March 2018, a US provider must disclose data in its "possession, custody, or control" wherever that data is stored, and that includes these logs.

Why it matters now

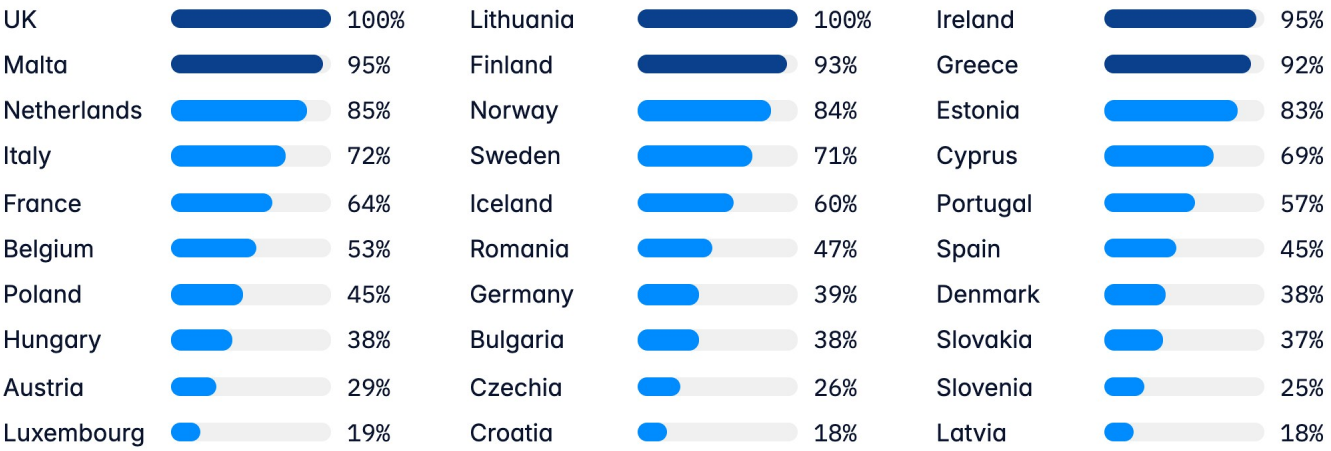
Sanctions reveal a second exposure: a US provider can be barred from serving a customer at all, and the effect travels through every US company in the supply chain.

2025–2026 After US sanctions on the ICC's chief prosecutor, his Microsoft email was disconnected. Microsoft told the UK Parliament in February 2026 that the ICC made that decision, then asked for the testimony to be corrected. The ICC has since moved to openDesk.

9 Oct 2026 The US designated the ICC as an institution. General licences permit core operations until 7 April 2027 and cover email and enterprise software.

26 Aug 2026 The US designated the Italian hosting collective Autistici/Inventati. Within days its .org domain was suspended, its payment account frozen, and its Italian bank account closed. It announced its shutdown on 6 September.

The UK and Lithuania run entirely on a US edge



The other side

We found no case of a CDN withdrawing service from a European government or broadcaster, and Microsoft France told the French Senate in 2025 that a compelled transfer of French data had never happened, although were unable to guarantee that it would never take place. The EU-US Data Privacy Framework covers personal data transfers, and several US providers offer EU-only processing, but neither removes the US parent's legal obligations. The proposed Cloud and AI Development Act would add a sovereignty assessment framework.

Finding 3

Nearly half of sites show no CDN protection

413 of 915 sites (45%) answer visitors directly from their own servers, with no CDN in front. Among government sites the figure is 59%.

A CDN caches pages close to visitors and absorbs traffic peaks. Without one, every request reaches the origin server. That matters most at the moments the sites are needed most: a storm warning, an election night, a tax deadline, or breaking news. It also matters during an attack. Most CDNs absorb network-level (Layer 3 and 4) floods and offer a web application firewall (WAF) that filters application-level (Layer 7) attacks such as HTTP floods, malicious bots, and injection attempts.

Tax authorities and CERTs are least likely to show CDN protection



Share of organisations in each function whose main site has no CDN at the edge.

Why It matters

DDoS is the most common attack these bodies face. ENISA's Threat Landscape 2026 analysed 8,257 incidents from 2025: DDoS made up 51% of them, public administration was the most targeted sector at 32%, and ideology-driven DDoS accounted for 82% of the events recorded against public administrations. ENISA also names dependence on third-party providers as a systemic risk.

The picture is polarised. Where European public bodies do use a CDN, 96% chose a US one. In practice the choice has been between US protection and no edge protection at all, partly because few European providers have built capacity to absorb multi-terabit attacks.

The other side

No CDN does not mean no protection. Many government hosting networks, including national data centres, may filter attack traffic upstream or run their own WAFs in ways an external scan cannot see, and ENISA describes most DDoS activity as low-impact and short-lived. But a site with no caching layer still has less headroom for a genuine surge in legitimate demand.

Compliance Map

Content delivery is a supply chain under NIS2

NIS2 already treats the CDN as part of an organisation's supply chain, and 17 October 2026 marked two years since the transposition deadline. Data protection, data access, and sovereignty rules now bear on the same layer.

Rule	What it requires	Date	Why it matters for content delivery
NIS2 Art 21(2)(c), (d), 21(3)	Supply-chain security and business continuity, taking into account the vulnerabilities and practices of each direct supplier	`18 Oct 2024`	The CDN is a direct supplier in the path of every request; one account covering a whole government is a concentration risk, and a failover under the same jurisdiction covers technical failure only
NIS2 Art 22, Recital 90	EU coordinated risk assessments of critical ICT supply chains, including non-technical factors such as undue third-country influence	`Ongoing`	Jurisdiction and sanctions exposure are recognised risk factors, not only technical ones
NIS2 Annex I	CDN providers listed as digital infrastructure; central government in scope as public administration	`18 Oct 2024`	Both the providers and most bodies in this study are covered, subject to Art 2(7) exclusions
CER Directive	Member states identify critical entities, which must then adopt resilience measures	`17 Jul 2026`	Continuity of public-facing services, including during supplier outages
GDPR Art 28, 44–49, 48	Processor guarantees and a lawful basis for third-country transfers; foreign court or authority orders recognised only under an international agreement	`In force`	Edge logs hold personal data, and with no EU-US CLOUD Act agreement a provider can face conflicting duties
Data Act Art 32	Data processing services must guard non-personal data against conflicting foreign government access	`12 Sep 2025`	Covers edge metadata that is not personal data
CRA Art 14	Report actively exploited vulnerabilities and severe incidents through ENISA	`11 Sep 2026`	Applies to the software inside self-built edges and caching layers
Cloud and AI Development Act	Proposed EU framework for assessing cloud sovereignty (Art 16, Art 29), with Union added value in procurement	`Proposed 3 Jun 2026`	Could give buyers a standard way to score delivery providers on jurisdiction
US CLOUD Act, FISA 702	US providers must disclose data in their control wherever it is stored (18 U.S.C. § 2713); FISA 702 permits surveillance of non-US persons	`CLOUD Act 2018; 702 lapsed 12 Jun 2026`	Applies to the providers behind 511 sites; 702 collection continues under a March 2026 certification

National NIS2 laws were due by 17 October 2024; Ireland, Spain, France, and the Netherlands were referred to the Court of Justice on 8 July 2026. NIS2 does not apply in the UK, and most private news publishers sit outside its scope; public broadcasters may be covered by national law. For news publishers, the case is resilience and protecting sources and readers, not compliance. Proposals are subject to change in negotiation. Informational only, not legal advice.

Recommendations

Considerations for public bodies and publishers

The findings do not imply leaving a current CDN provider. They point to understanding the dependency and planning for a fallback.

1 **Map the edge**

List providers in the delivery path, including government platforms, asset hosts, and APIs, and record each one's legal jurisdiction, where its logs are kept, and who controls its configuration.

2 **Assess the CDN as a NIS2 supplier**

Treat the CDN provider as a direct supplier under Article 21(2)(d) and 21(3), covering concentration, jurisdiction, sanctions exposure, and exit terms.

3 **Build a second path**

A second CDN, a provider under a different jurisdiction, or extra origin capacity keeps the site up if one provider fails or withdraws service.

4 **Protect crisis sites for peak demand**

Civil protection, police, and tax sites need caching and DDoS protection sized for their busiest day, and a web application firewall against application-level attacks.

5 **Keep control of configuration and logs**

Keep delivery configuration and request logs under your own control and jurisdiction, so EU law governs access to them.

6 **Write sovereignty into procurement**

Add jurisdiction, portability, and exit criteria to tenders, including where an integrator chooses the CDN, and align them with the EU cloud sovereignty framework once it is adopted.

About

Method, scope, and disclosure

We identified the provider and legal jurisdiction behind the websites of 1,122 government bodies and news organisations in 30 European countries, using only public signals: DNS records, network ownership, and HTTP response headers.

Sample

The 27 EU member states, the UK, Norway, and Iceland. Government (745): national portals, every ministry on official government lists, national CERTs, police, tax authorities, civil protection agencies, and shared government platforms. Media (377): European Broadcasting Union members, national news agencies, and the top 10 news sites per country from national audience measurement. Several bodies share one site, so headline figures count 915 unique websites.

Detection

For each organisation we resolved the primary domain, the main site's host after redirects, and up to eight asset and API hostnames: 4,705 hostnames in total. Each was classified from its DNS chain, network owner (ASN), and the response headers of one HTTPS request. Trackers, consent tools, and video streaming hosts were excluded.

Confidence

605 organisations were classified with high confidence (a CDN-specific DNS record or header), 482 medium (a CDN-only network), and 35 low (a general cloud network without CDN headers).

Definitions

"US-headquartered" refers to where the provider is headquartered, not where data is stored, and includes 26 sites served directly from US cloud platforms without a CDN. "No CDN" means no CDN signal at the edge; a site may still have network-level protection that an external scan cannot see.

Limits

Results reflect one vantage point (Sweden) on 12 and 13 October 2026. Some sites block automated requests, and DNS-based traffic steering can give different answers elsewhere. Jurisdiction is a legal exposure, not evidence that any data access has occurred.

Conduct

One homepage request per site plus one request per hostname, with no crawling, port scanning, or collection of personal data.

Disclosure

This research was carried out by Varnish Software, which develops content delivery and caching software, including a European CDN. The dataset and per-country figures are available to journalists and researchers on request, so that every classification can be checked independently.

Appendix

Sources

Varnish research dataset: CDN usage by European government and media organisations	12–13 October 2026
Directive (EU) 2022/2555 (NIS2) and Directive (EU) 2022/2557 (CER), EUR-Lex	
Regulation (EU) 2016/679 (GDPR), Regulation (EU) 2023/2854 (Data Act), and Regulation (EU) 2024/2847 (CRA), EUR-Lex	
European Commission, proposal COM(2026) 502 for a Cloud and AI Development Act	3 June 2026
18 U.S.C. § 2713 (CLOUD Act), Cornell Legal Information Institute	
Congressional Research Service, The Impact of FISA Section 702's Repeal, LSB11444	22 June 2026
US Treasury OFAC, International Criminal Court-related General License No. 13	9 October 2026
Global Sanctions, US designates International Criminal Court	9 October 2026
The Record, Autistici/Inventati shuts down after US terrorist designation	September 2026
The Next Web, Italian hosting collective Autistici/Inventati is shutting down	September 2026
The Register, Microsoft admits it 'cannot guarantee' data sovereignty	25 July 2025
The Register, Microsoft asks UK Parliament to correct ICC testimony	18 February 2026
Scottish Legal News, ICC to ditch Microsoft following US sanctions	3 November 2025
The Register, Europe picks 4 sovereign cloud providers	20 April 2026
WilmerHale, European Court of Justice to review challenge to the EU-US Data Privacy Framework	1 December 2025
Cloudflare, Cloudflare outage on February 20, 2026 (postmortem)	February 2026
Cloudflare, Cloudflare outage on November 18, 2025 (postmortem)	November 2025
Amazon Web Services, Summary of the Amazon DynamoDB service disruption	October 2025
Taiwan News and MaltaToday, reporting on the Cloudflare outage of 18 November 2025	November 2025
ENISA, Threat Landscape 2026	22 September 2026
Help Net Security, Europe's technology backbone is becoming a cyber target	24 September 2026
Law Society Gazette Ireland, Ireland referred to CJEU over cyber bill	8 July 2026
Hunton Andrews Kurth, Commission refers four member states to CJEU over NIS2 transposition	July 2026