nederlandse
publieke
omroep

# Publieke media en souvereiniteit

Dutch Guild 12 mei 2026

# Even kennismaken

Walter Leemhuis

- Hilversum: 1 vrouw, 2 dochters, enkele gitaren
- Rabobank: Security Operations Center + ISO betalingsverkeer
- Politie: Delivery mgr Security Services
- Defensie: Technisch Verantwoordelijke Informatiebeveiliging
- 2023 NPO, CISO en Techlead Security Operations
- Aktief in Platform voor Informatiebeveiliging (PvIB)

# Over de NPO

Overkoepelende taken van de NPO voor de omroepen

- Technische distributie en uitzending van al het aanbod
- Toegankelijk maken van programma's voor mensen met een gehoor- of visuele beperking
- Beheer van streamingdiensten als NPO Start en NPO Luister
- Beheer van rechtencontracten
- Aankoop van buitenlandse films en series
- Verkoop van eigen formats
- Publieksonderzoek
- Zorgen voor eenduidige metadata (programmagegevens) en verspreiding daarvan
- Marketing voor alle NPO-kanalen

Evaluatie onafhankelijke commissie Publicatie 11-05-2026

# ‘Focus op de kernwaarden – Evaluatie van de Nederlandse publieke omroep’

**Existentiële uitdaging voor de Nederlandse publieke omroep**

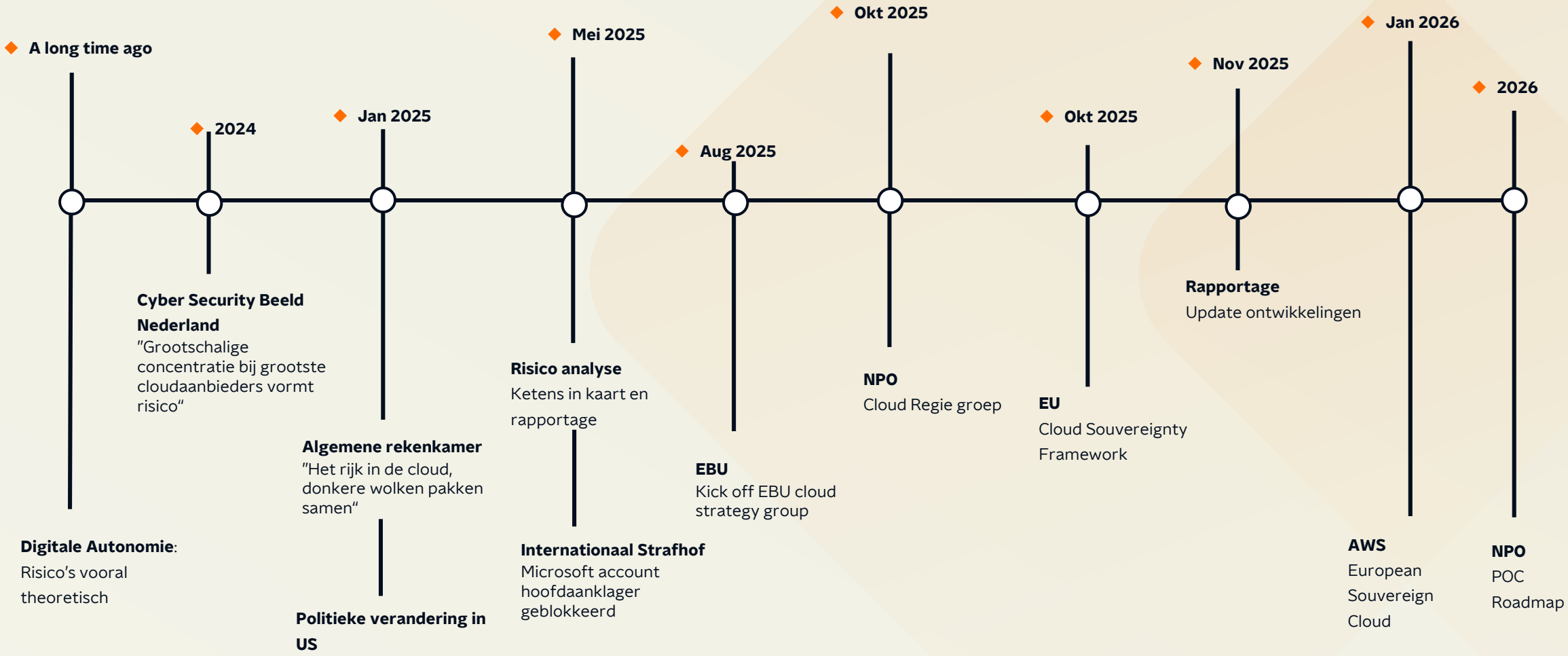
De commissie signaleert dat het Nederlandse publieke omroepbestel zich bevindt op een kritiek punt in zijn levensloop. Hij is onderhevig aan grote bedreigingen van buitenaf.

Het medialandschap is ingrijpend veranderd en wordt bepaald door digitalisering en Big Tech. Platforms als YouTube, Facebook, TikTok en Netflix hebben een poortwachtersfunctie gekregen en bepalen in toenemende mate wat Nederlanders zien, horen en geloven. Zij beïnvloeden het debat via algoritmes die niet zijn ontworpen voor democratische waarden, maar voor maximale aandacht, data verkrijging en winst. In dat krachtenveld verliest de publieke omroep terrein.

Dit speelt zich af binnen een geopolitieke context waarin in steeds meer landen autocratische tendensen toenemen en publieke omroepen hun onafhankelijkheid en betrouwbaarheid dreigen te verliezen.

De commissie vindt deze context dermate alarmerend, dat zij spreekt van een existentiële uitdaging voor de publieke omroep.

# Ontwikkelingen op een rijtje



# Risico Analyse

- Beschikbaarheid Integriteit Vertrouwelijkheid
- Primair op uitzendkritische processen
- Ondersteunende bedrijfsprocessen kantoorautomatisering, Financien, HR
- Financien (denk ook handelsbazooka)

- Herzie Cloudstrategie
- Maak exitplannen
- Onderzoek europese aanbieders
- Realiseer een noodvoorziening
- Migratie naar Europa voor systeem waar privacy meest belangrijk is

# EBU Cloud strategy group

Met dank aan Frans de Jong voor de komende slides!

Help EBU members to adopt effective, flexible, resilient, sovereign, and sustainable (multi)cloud solutions

# The Problem in Plain Terms

*How did the media end up inside someone else's infrastructure?*

## What happened?

Over the past decade, public service media have migrated large parts of their production and distribution pipelines to cloud services operated by a handful of US-based companies — Amazon (AWS), Google, Microsoft Azure.

This was driven by cost savings, AI capabilities, and the speed of innovation those platforms offer.

The European Media Freedom Act (EMFA) does not mention infrastructure at all.

## Why does it matter?

### Editorial control

Who controls the **infrastructure** may influence what gets published, amplified — or blocked. Mainly AI (e.g. bias) and online platforms related, rather than production infrastructure?

### Legal exposure

US CLOUD Act can compel access to data held on US-owned servers, even in Europe. Especially relevant for investigative journalism.

### Operational fragility

A policy change, price hike, or geopolitical event by one vendor can halt news production overnight.

### Democratic risk

Nov 2025: Dutch media chiefs wrote to government warning of a threat to 'democratic resilience and national security'.

# Who Are the Hyperscalers?

*A non-technical explainer — think of them as landlords of digital infrastructure*

*Analogy: Imagine outsourcing your entire newsroom — servers, editing suites, archives, email, even the AI that writes captions — to a single landlord. You pay rent, use their tools, and depend on their rules. That is what cloud dependency looks like.*

| AWS (Amazon) | Microsoft Azure | Google Cloud |
|---|---|---|
| Largest cloud provider globally. Powers streaming, storage, AI for many European broadcasters. Offers 'European Sovereign Cloud' but remains US-controlled. | Deep integration with newsroom software (Teams, Office 365). Azure for Operators serves media. 'Cloud for Sovereignty' is a partial answer. | AI and ML powerhouse. YouTube infrastructure. Many PSMs use Google for content delivery and analytics. 'Sovereign Cloud' initiative exists. |

Together these three companies control over 60% of the global cloud infrastructure market (Synergy Research, Q3 2025). For European PSM, they are the default.
Note: this slide focuses on US hyperscalers, but we should not exclude Asia — the strongest example is Alibaba Cloud (IOC Olympic Games partner since 2017). The EBU Group uses ‘non-European’.

# The EBU Strategic Response

*Four 'Strategic Beacons' — a roadmap from dependency toward managed sovereignty (EBU TR 099)*

*The EBU does not advocate for full exit from hyperscalers. Instead, TR 099 proposes a 'managed hybrid' approach that progressively builds European alternatives while maintaining operational continuity and freedom of choice.*

## Cloud-First

Every new technology investment defaults to evaluating cloud-native solutions first — but cloud does not mean hyperscaler. We advocate Freedom of Choice.

The risk assessment differs between broadcasters (and governments!). It makes a big difference if you are primarily concerned with the latest innovations or disaster recovery. So, horses-for-courses, but a strong appeal to 'Think Cloud' (can be on-premises) first. Hybrid architectures can keep mission-critical operations on-premises (live studios, emergency broadcast, …).

## Proactive Sovereignty

Sovereignty is not just where data is stored. It covers data control, operational independence, legal jurisdiction, and technical portability. The EBU proposes a sovereignty decision matrix to classify workloads by risk — protecting journalistic sources and editorial independence most rigorously.

## Partnership Advantage

No single PSM can negotiate with AWS on equal terms. Collectively, EBU Members have the potential to pool purchasing power, co-develop frameworks, and negotiate contractual safeguards (sovereignty guarantees, exit rights, audit clauses) that individual organisations cannot obtain alone. Thinking beyond the EBU domain increases leverage. E.g. the UK public sector alone awarded £3.8bn across 1,809 AI contracts (2018-2026), dominated by Microsoft, Palantir & Deloitte (Tussell AI Procurement Tracker, Mar 2026).

We are currently investigating how far Members want to go with this and of course what the legal limitations are.

## Shared Solutions

European PSMs can share more. Common requirements for frameworks/APIs (e.g. TAMS, MXL) or concrete solutions; When one PSM or vendor builds something that works — a transcoding pipeline, a media asset workflow, an AI tool — the larger ecosystem could benefit from it. We do not need to create the same thing 10s of times in each country. Solutions need not be built by EBU Members to be shared through the EBU family.

A concrete first step is opening up the results of PoCs to other Members.

# Why Disentangling Is Hard

*Technical, economic, and organisational barriers*

**The honest technical answer: full disentanglement from hyperscalers is currently not feasible for most European PSMs. Here is why.**

### Vendor Lock-in

Hyperscaler services use proprietary APIs, data formats, and toolchains. Migrating away requires rewriting applications, retraining staff, and rebuilding integrations — a multi-year, multi-million-euro project.

### AI Dependency

State-of-the-art AI for transcription, translation, content tagging, and recommendation is available from hyperscalers. No European provider matches AWS Bedrock, Azure OpenAI, or Google Vertex at scale today.
Alternative models exist (Whisper, Llama, Mistral); the lock-in is the managed-service convenience — APIs, auto-scaling, SLAs — not so much in the models themselves.

### Cost Asymmetry

Hyperscalers benefit from global economies of scale. A ~10–30% premium (McKinsey 'Sovereign AI', Mar 2026) applies to hyperscalers' 'sovereign' configurations. PSMs face budget pressure, so workload-by-workload selection matters.

By the way: EU-native providers are often cheaper than hyperscalers on commodity compute, storage and egress (list prices), but hyperscalers offer deep enterprise discounts.

### Skills Gap

Internal cloud expertise in PSMs is often built around AWS or Azure tools. Retraining or replacing that expertise takes years and competes with private sector salaries.

### Legacy Systems

Many PSMs still run 20-year-old broadcast infrastructure alongside cloud services. Hybrid integration — not clean migration — is the operational reality for the foreseeable future.

### Contractual Inertia, Risk Perception

Long-term licensing agreements, SLAs, and deeply embedded software ecosystems (e.g., Microsoft 365 in every newsroom) mean switching costs are not just technical — they are legal and contractual.

Risk perception often is different within a company. From 'Wait 2 years' to 'protect my investigative journalism source now".

Hardware dependency: cloud and on-prem alike rest on a tiny handful of originators — Nvidia for AI accelerators, TSMC for leading-edge chip fabrication, ASML (NL) for EUV lithography. Sovereignty at the silicon layer is even narrower than at the cloud layer.

# The European Alternative Landscape

*Alternatives exist — but the gap with hyperscalers is real and must be named honestly*

### EU-Native Cloud Providers

*OVHcloud (FR) · STACKIT (DE) · Scaleway (FR) · IONOS (DE) · Exoscale (CH) - …*

Operated under EU law and ownership. Comply with GDPR, NIS2, EU Data Act. Preferred by EBU for workloads requiring full European sovereignty. Capabilities are growing but still narrower than hyperscalers — especially in frontier AI and global delivery.

### Hyperscaler 'Sovereign' Offerings

*AWS European Sovereign Cloud · Microsoft Cloud for Sovereignty · Google Sovereign Cloud*

Designed to meet EU requirements for data residency and operational control. May satisfy compliance needs but legal jurisdiction ultimately remains with a US parent company. The U.S. CLOUD Act exposure is not fully eliminated.

### Member / National Private Clouds

*On-premises data centres · National telco clouds · PSM-owned (also non-Cloud) infrastructure*

Full control. Ideal for live production, and emergency, on-site broadcast. High cost, limited scalability. The EBU model keeps these for 'mission-critical' and latency-sensitive workloads, not general-purpose cloud compute.

*Takeaway: the European cloud landscape is maturing — but today no single European provider replaces AWS, Azure, or Google. The answer is a hybrid, not a single alternative.*

# In gesprek met de Business

**Objectieve criteria op basis van EU model**

EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR DIGITAL SERVICES

Luxembourg

| Sovereignty Effectiveness Assurance Levels | Sovereignty Effectiveness Assurance Levels Descriptions |
|---|---|
| **SEAL-0** | *No Sovereignty*:<br>Service, technology or operations under **exclusive control of non-EU third parties**, governed entirely in **non-EU jurisdictions**. |
| **SEAL-1** | *Jurisdictional Sovereignty*:<br>**EU law formally applies** with **limited practical enforceability**; service, technology or operations under exclusive control of non-EU third parties. |
| **SEAL-2** | *Data Sovereignty*:<br>**EU law applicable and enforceable**, with **material non-EU dependencies remaining**; service, technology or operations under indirect control of non-EU third parties. |
| **SEAL-3** | *Digital Resilience*:<br>**EU law applicable and enforceable**, EU actors exercising **meaningful but not full influence**; service, technology or operations under marginal control of non-EU third parties. |
| **SEAL-4** | *Full Digital Sovereignty*:<br>Technology and operations under **complete EU control**, subject only to **EU law**, with **no critical non-EU dependencies**. |

| # | Sovereignty Objectives | Weight in Scoring |
|---|---|---|
| **SOV-1** | **Strategic Sovereignty** | **15%** |
| **SOV-2** | **Legal & Jurisdictional Sovereignty** | **10%** |
| **SOV-3** | **Data & AI Sovereignty** | **10%** |
| **SOV-4** | **Operational Sovereignty** | **15%** |
| **SOV-5** | **Supply Chain Sovereignty** | **20%** |
| **SOV-6** | **Technology Sovereignty** | **15%** |
| **SOV-7** | **Security & Compliance Sovereignty** | **10%** |
| **SOV-8** | **Environmental Sustainability** | **5%** |
| | **Total** | **100%** |

# Werkbaar Sjabloon

| Zekerheidsniveau (SEAL level) | Uitleg | Praktische maatregelen |
|---|---|---|
| **0 - Geen Souvereiniteit** | Verrichtingen onder exclusieve zeggenschap van derde landen van buiten de EU, volledig in niet-EU-rechtsgebieden | Standaard Cloud/SAAS overeenkomst bijvoorbeeld AWS, Google of Azure |
| **1 - Jurisdictiesoevereiniteit** | Beperkte praktische afdwingbaarheid; service, technologie of transacties onder exclusieve zeggenschap van derden van buiten de EU | Standaard Cloud overeenkomst met extra juridische waarborgen. Zoals Standard Contractual Clause, data-locatie en verwerkersovereenkomst |
| **2 - Gegevenssoevereiniteit** | EU-wetgeving toepasselijk en beperkt afdwingbaar, met resterende materiële afhankelijkheden van buiten de EU | Diensten op Standaard Cloud maar bedrijfsgevoelige data en persoonsgegevens onder EU wettelijk gezag |
| **3 - Digitaal weerbaar** | EU-wetgeving van toepassing en betekenisvol afdwingbaar. Dienstverlening, technologie en activiteiten onder marginale controle van niet-EU-derden | Service en bedrijfsgevoelige data en persoonsgegevens onder afdwingbaar EU rechtsregime. Niet gevoelige data via standaard Cloud overeenkomst |
| **4 - Volledige digitale soevereiniteit** | Technologie en operaties onder volledige EU-controle, uitsluitend onderworpen aan het EU-recht, zonder kritieke afhankelijkheden buiten de EU. | Diensten en alle data fysiek in EU en onder afdwingbaar EU rechtsregime. Non EU partijen uitgesloten |

# Kies SEAL level per objective

| onderdeel | Soevereiniteit: | Korte omschrijving | Relevantie voor NPO, wat bespreken we | Bijdragende factoren aan score | Kies minimum SEAL level |
|---|---|---|---|---|---|
| SOV 01 | Strategisch | De mate waarin de provider verankerd is in het juridische, financiële en industriële ecosysteem van de EU (bv. eigendomsstructuur, bestuur denk aan overname Digid door US partij). | De mate van autonomie waarin NPO directie en bestuur controle heeft en zelfstandig beslissingen kan nemen. Voor primaire processen van belang secundaire minder belang | Ervoor zorgen dat organen met beslissende bevoegdheid over uw diensten zich binnen de jurisdictie van de EU bevinden.<br><br>Beoordelen van de garanties met betrekking tot wijzigingen in zeggenschap (change of control).<br><br>De mate waarin de aanbieder afhankelijk is van financiering uit EU-bronnen.<br><br>De omvang van investeringen, werkgelegenheid en waardecreatie binnen de EU.<br><br>Betrokkenheid bij EU-initiatieven en consistentie met de digitale, groene en industriële soevereiniteitsdoelstellingen die op EU-niveau zijn vastgesteld.<br><br>Het vermogen om veilige operaties voort te zetten bij verzoeken om de dienstverlening te staken of op te schorten, of wanneer ondersteuning van de leverancier wordt ingetrokken of verstoord | SEAL-3 (Digitaal weerbaar): EU-actoren hebben zinvolle invloed, maar er is nog steeds marginale controle door niet-EU-partijen. |
| SOV 02 | Juridische | De blootstelling aan buitenlandse wetgeving (zoals de US Cloud Act) en de afdwingbaarheid van Europese rechten. | De mate waarin NPO buitenlandse wetsregimes Accepteert. Waarbij EU wetgeving mogelijke ondergeschikt wordt<br><br>*Is gemaakte keuze uitlegbaar,*<br>*Heeft het effect op reputatie NPO?* | Het nationale rechtssysteem dat van toepassing is op de activiteiten en contracten van de aanbieder.<br><br>De mate van blootstelling aan niet-EU-wetgeving met grensoverschrijdende reikwijdte (bijv. de Amerikaanse CLOUD Act, de Chinese Cybersecurity Law).<br><br>Het bestaan van juridische, contractuele of technische kanalen waarlangs niet-EU-autoriteiten toegang tot data of systemen kunnen afdwingen.<br><br>De toepasbaarheid van internationale regelgevingen die het gebruik of de overdracht kunnen beperken.<br><br>De locatie waar intellectueel eigendom wordt gecreëerd, geregistreerd en ontwikkeld (EU versus derde landen), evenals de juridische jurisdictie die van toepassing is op de creatie en ontwikkeling van het intellectueel eigendom. | SEAL-2 (Gegevens soevereiniteit): EU-recht is afdwingbaar, maar er blijven materiële niet-EU-afhankelijkheden bestaan |

# Tot slot, hoe nu verder

- Souvereiniteit inbedden in
  - Inkoopproces
  - Operationele processen/Architectuur
- Cloud Center of expertise
- Contracteren EU partij
- Roadmap Uitwerken
  - Presenteren
  - Budgetteren 2027 en verder
- Ambitie uitgesproken verhuizing NPO-id
- Live brengen en beheren noodvoorziening
- Keuze werkomgeving->POC nextcloud.