RESEARCH REPORT

National Support Structures and Capabilities for growing Digital Sovereignty through Sharing and Reuse of Open Source Software in the Public Sector

A report commissioned by the Danish Agency for Digital Government (Digitaliseringsstyrelsen) and Local Government Denmark (KL)

RISE RAPPORT 2026:38

Johan Linåker, RISE

National Support Structures and Capabilities for growing Digital Sovereignty through Sharing and Reuse of Open Source Software in the Public Sector

JOHAN LINÅKER

This work is licensed under CC BY 4.0 https://creativecommons.org/licenses/by/4.0/

Abstract

National Support Structures and Capabilities for growing Digital Sovereignty through Sharing and Reuse of Open Source Software in the Public Sector

Denmark faces a growing need to strengthen digital sovereignty as dependencies on dominant technology vendors limit choice, transparency, and long-term control over critical digital infrastructure. Open Source Software (OSS) emerges as a practical lever to address these challenges, enabling greater autonomy, interoperability, and shared innovation across the public sector. However, Danish public-sector organisations currently lack the common capabilities required to adopt, steward, and collaborate effectively on OSS at scale. Years of outsourcing, fragmented procurement practices, and uneven technical maturity have created structural barriers that hinder reuse and collective development.

This report proposes a federated national support structure based on Open Source Program Offices (OSPOs) operating at national, regional, municipal, and institutional levels. The model combines policy translation, procurement and compliance support, shared digital collaboration infrastructure, community stewardship, training, and cross-government coordination. It emphasises proximity-based support, reusable artefacts, and scalable governance, organised through a national OSPO network, anchored in a National Government OSPO that provides strategic direction, shared tools, and alignment with European initiatives.

A phased maturity model outlines how Denmark can move from today's fragmented efforts to a coherent ecosystem where OSS and open collaboration are embedded practices. Through coordinated investment, strengthened stewardship, and long-term capability building, Denmark can enhance digital sovereignty while fostering transparency, resilience, and sustainable innovation across the public sector.

Keywords: Digital Sovereignty, Strategic Autonomy, Digital Resilience, Open Source Software, Software Reuse, Policy, Open Source Program Office, Public Sector, Public Administration, Open Government

RISE Research Institutes of Sweden AB

RISE Report 2026:38
ISBN: 978-91-90109-67-0

Executive summary

European sense of urgency for digital sovereignty

Across Europe, governments are becoming more digitally interconnected while awareness is growing regarding the lack

of control over the technologies that underpin public services (Folketinget, 2025). Long-standing dependencies on a small number of dominant vendors across hardware, cloud and software have reduced choice, escalated costs, and introduced new geopolitical and security risks (Di Marco et al., 2025; Edler et al., 2023). Digital sovereignty has therefore become a central European policy priority, emphasising the ability to design, govern and sustain key digital technologies on domestic terms (European Parliament, 2026; von der Leyen, 2026).

For Denmark, digital sovereignty is considered a major concern and priority (Folketinget, 2025), with calls for increased promotion and growth of choice and competition, as well as investments into pilots to grow experience and capabilities (Regeringen, KL, & Danske Regioner, 2025). Recent analysis further strengthens concerns regarding the lack of control, governance, and transparency over data and software, as well as the cybersecurity and geopolitical risks that accompany them (PA Consulting, 2026).

Open source software provides a lever – but requires new capabilities

The same analysis further centres attention to Open Source Software (OSS) as a key tool for enabling and promoting digital sovereignty and innovation, something also echoed across research (Blind et al., 2021; Edler et al., 2023), ministerial declarations (European Commission, 2017a, 2020a, 2022), and more recently in EU's coming sovereignty package, including an EU-level OSS strategy, and the Cloud and AI Development Act (European Commission, 2026). However, the ability to leverage OSS strategically requires common capabilities that many Public-Sector Organisations (PSOs) in Denmark do not currently possess. Years of outsourcing have eroded internal technical competence, procurement practices remain risk-averse, and political support is inconsistent. With current policy concerns in mind, there is now an opportunity to address this gap and to see new capabilities emerge that enable Denmark to fully leverage the potential of open technologies and innovation in shaping its digital future.

Open Source Program Offices – a vehicle for change management

Adoption of OSS at a strategic level (i.e., as a means of achieving overarching strategic goals, such as digital sovereignty) essentially requires organisational and cultural change, as well as support structures to advise and execute the strategy (Linåker & Muto, 2024). In response, an organisational construct referred to as Open Source Program Offices (OSPOs) has emerged, originally from the software industry shortly after OSS was introduced (Ruff, 2022).

The OSPOs provide support for their respective organisations (European Commission, 2020b), helping to accelerate organisational readiness and to grow capabilities to adopt, develop, and collaborate on OSS to reach the organisation's strategic goals (Digitaliseringsstyrelsen, 2025). Essentially, the OSPOs act as change agents in their

respective contexts, working to onramp cultural mindsets and ways of working into the open innovation paradigm (Linåker et al., 2024). Each OSPO will look different and be shaped by the conditions and goals of the overarching organisation. Still, there are overlaps, and a joint best practice has emerged from industry as goals commonly converge, including supply-chain control and market power.

The OSPO construct is now increasingly adopted internationally, including in the public sector across Europe, addressing needs for digital sovereignty while enabling the potential innovation and economic upside that OSS offers (Linåker & Muto, 2024). The Centre for Digital Sovereignty (ZenDIS) in Germany and the regional OSPO of Schleswig-Holstein are two prominent examples (PA Consulting, 2026), while several others have been studied at the national, regional, and local levels of government (Linåker et al., 2024). These include single governments and PSOs, as well as association-based OSPO structures where PSOs collaborate and pool resources through a co-owned entity (Digitaliseringsstyrelsen, 2025). In cases where governments lack the resources and political will, civil society has been found to provide complementary support structures. Academic OSPOs have also been reported across Institutes for Research and Higher Education.

The OSPO as a driver for digital sovereignty in Denmark

In this report, commissioned by Local Governments Denmark (KL) and the Danish Agency of Digital Government (Digitaliseringsstyrelsen), we consider the specific context of Denmark, and how its governments and PSOs can grow the capabilities necessary to enable sharing and reuse of OSS, grow a strategic autonomy (Edler et al., 2023), and exploit the innovation opportunities OSS provides (Blind et al., 2021).

Specifically, we build on the recommendation from the analysis of digital sovereignty in the Danish public sector, which proposes establishing a national centre for digital sovereignty and innovation (PA Consulting, 2026). Using the OSPO construct (Digitaliseringsstyrelsen, 2025), we aim to propose a design and strategy for the consideration and implementation of public-sector OSPOs that can support incentives and policy goals related to digital sovereignty in Denmark.

Through this study, we ask and address the following questions:

- RQ1: How are strategic goals and vision in terms of digital sovereignty and potential opportunities of cross-government collaboration, sharing and reuse of OSS solutions characterised among Danish PSOs?
- RQ2: What are the central barriers for cross-government collaboration, sharing and reuse of OSS solutions among Danish PSOs?
- RQ3: What capabilities are required for cross-government collaboration, sharing and reuse of OSS solutions among Danish PSOs?
- RQ4: How can the identified capabilities be enabled and realised through public-sector OSPOs in Denmark?

Digital sovereignty, interoperability and cost efficiencies core incentives

Interviews show a clear shift from viewing OSS primarily as a tool for vendor independence to understanding it as a practical instrument for digital sovereignty. OSS

provides the power and freedom to switch and adapt systems, ensures credible exit options, and strengthens control over data and infrastructure. Innovation and interoperability are added value, with open standards and OSS enabling efficient data exchange and cross-government reuse. Cost and efficiency reinforce the case, as shared development reduces duplication, lowers operating expenses and strengthens the domestic and European supplier ecosystem.

(For further reading, see section 4)

Structural barriers and legacy culture hinder change

Progression towards policy goals and potential benefits is, however, hindered by structural barriers present across the public sector. Strategic misalignment leads to parallel efforts and inconsistent leadership support. A procurement culture shaped by dominant vendors reinforces lock-in and makes it difficult to mobilise early funding for OSS alternatives. Many PSOs lack the organisational and technical capabilities needed to adopt, maintain or contribute to OSS after years of outsourcing. Concerns about usability, security and operational risk further slow uptake, with short-term productivity perceptions often outweighing long-term benefits in flexibility, resilience and sovereignty.

(For further reading, see section 5)

Growing diverse and interconnected capabilities

Addressing challenges highlighted requires a coordinated set of capabilities that together form the foundation for a national OSS support structure:

Policy translation and strategic advice – Interpreting EU legislation and national priorities, and helping develop OSS strategies and governance models, while aligning cross-government policies on OSS and related areas and topics, including cloud, AI, data governance and security.

Design and operationalisation of policy instruments – Guiding when source code ownership is needed, and how necessary control mechanisms can be created including and beyond OSS; providing procurement guidance and hands-on support, while maintaining essential templates and resources; enabling decision-making for OSS release; supporting project initiation and community development; strengthening sustainability and supply-chain risk management; and preparing organisations for emerging areas such as open source AI, and use of Agentic AI-support in software development.

Investment, prioritisation and scaling - Facilitating and promoting strategic seed funding and impact demonstration, as well as maintenance funding for critical digital infrastructure; developing prioritisation frameworks and migration pathways, and enabling joint agreements and coordinated rollouts.

Shared digital collaboration infrastructure – Establishing, growing, and governing a national government social code collaboration platform and OSS solution catalogue with related communities, templates, resources, on-ramps and taxonomies.

Licence compliance management - Providing routines, tools and guidance to ensure compliant OSS intake, SBOM-based monitoring, pre-release checks and ongoing auditability.

Stewardship of public-sector OSS projects - Ensuring long-term sustainability and shared governance through association-based, supplier-based, internal, or state-owned stewardship models.

Measurement and follow-up - Tracking adoption, reuse, project health, and compliance to guide risk management, improve infrastructures, and inform iterative policy refinement.

Inner Source enablement - Supporting internal and cross-government code sharing and collaboration to build open-working habits before full external release is feasible; enabling government-internal sharing of assets deemed unfit for open dissemination and reuse.

Advocacy and community building - Driving cultural change, building trust, and convening communities of practice across PSOs, suppliers, and civil society to normalise OSS collaboration.

Training and competence development - Providing role-specific capability building and training for policymakers, procurement officers, developers, legal teams, security specialists and end-users.

(For further reading, see section 6)

A structure that fits Denmark's decentralised governance

A comprehensive support structure is needed to develop and provision such capabilities, and must reflect Denmark's decentralised, multi-actor public sector while strengthening national coherence. The analysis shows the value of building on and leveraging existing actors and distributing responsibilities across national, regional and local levels rather than concentrating them in a single entity. Any OSPO needs positioning where mandate, authority, and trust-based relationships align, along with presence of, and close feedback-loops from technical capabilities and standardisation efforts. Staffing with socio-technical OSS expertise and community-trust as key competencies are crucial for success. Strategic guidance must be paired with practical enablers such as catalogues, templates, shared platforms and procurement support. Internal capability building must progress alongside cross-government collaboration, supported by strong communication and change management functions. Sustainable stewardship models are required to maintain shared OSS solutions over time. Stable funding for both new alternatives and critical maintenance, combined with reusable artefacts and automation, is essential for scaling adoption.

(For further reading, see section 7.1)

Comparing organisational models for open source support

Three organisational models were assessed. A *centralised* model provides clarity but does not match the diversity and autonomy of Denmark's public sector. A *decentralised* model provides flexibility but results in fragmentation and uneven capacity. A *federated* model, with national, regional, and local OSPOs supported by shared

infrastructure and coordinated governance, offers the most resilient, scalable, and context-appropriate architecture.

(For further reading, see section 7.2)

A federated model for national, regional and local support

Considering the characteristics and needs, the report presents a pragmatic, federated support structure for Denmark. The model reflects the Danish governance context - decentralised, multi-actor, and capability-uneven - while drawing on empirical lessons from European reference cases. It is designed to grow and coordinate the capabilities necessary for public-sector OSS adoption, reuse, collaboration, and stewardship, as detailed in Section 6, and to connect these capabilities across levels of government through a coherent national OSPO network.

The structure comprises and depends on several building blocks:

- *A National Government OSPO* hosted by the Agency of Digital Government, anchoring policy translation, national instruments, shared infrastructures, and cross-government coordination.
- *A Regional Government* OSPO providing coordinated support for the five regional governments, hosted by one of the Regions, or through a common-owned entity.
- *An Association-based OSPO* through OS2 providing proximity support, localisation of guidance, and aggregation of municipal needs.
- *Local Government OSPOs* are embedded where needs and capacity align in local governments, and are focused on internal governance, intake/release processes, and developer enablement.
- *Institution-centric OSPOs* are embedded where need and capacity align in single PSOs (regardless of the level of government), and are also focused on internal governance, intake/release processes, and developer enablement.
- *Supporting national functions*, including stewards, a project brokerage, procurement bodies, and funding programmes, that ensure the long-term sustainability, discoverability, and operationalisation of shared OSS projects.

Together, these entities form a distributed yet coordinated ecosystem capable of delivering the technical, organisational, and policy-related support that Denmark requires to scale OSS-based collaboration and improve digital sovereignty.

(For further reading, see section 7.3)

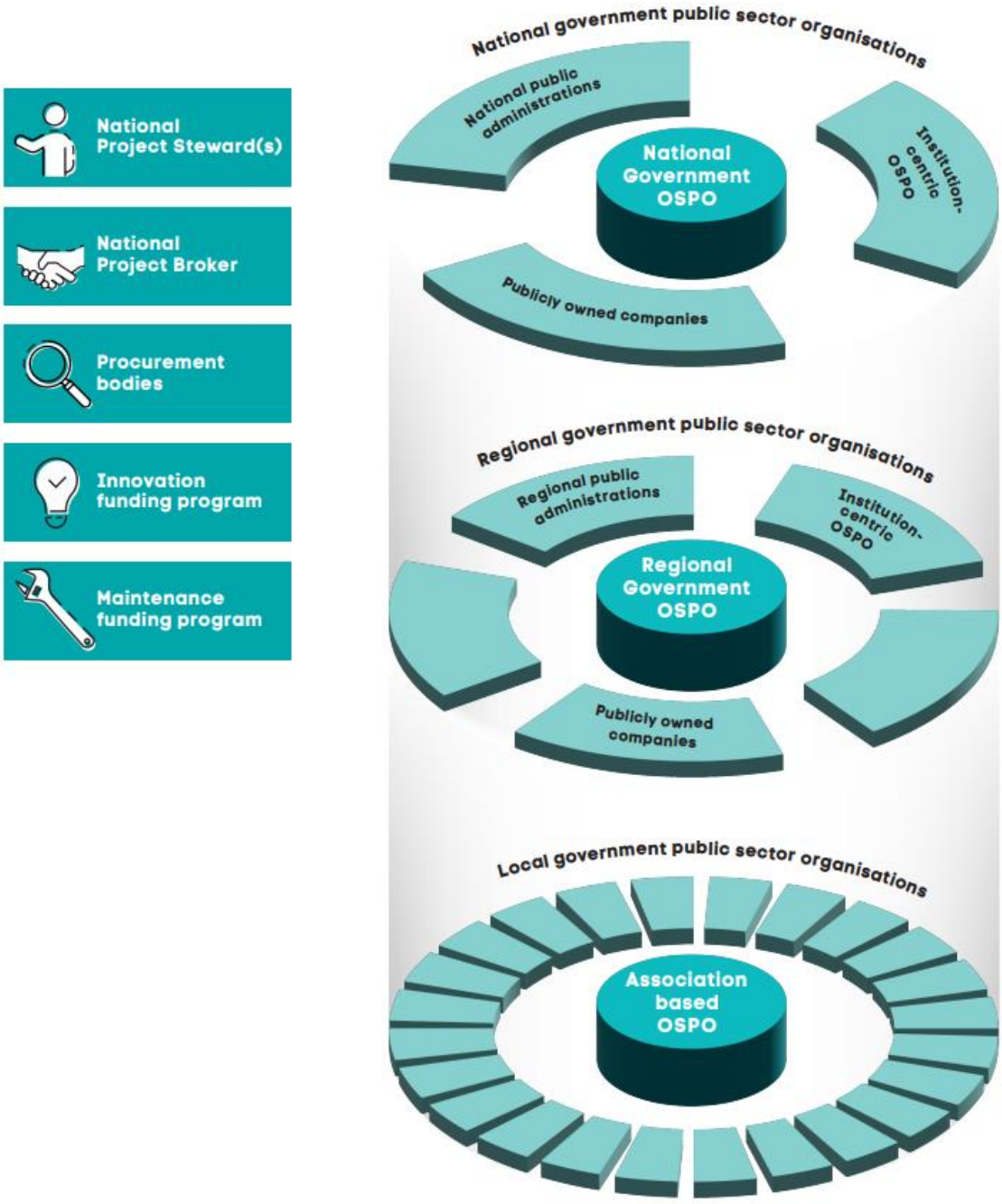

Figure 1: Overview of the national support structure, including the National Government, Regional Government and Association-based OSPOs supporting the national, regional and local levels of government respectively. Institution-centric OSPOs may be present across all levels. Local government OSPOs occur within single resourceful municipalities. National support functions as the National Project Steward and Project Broker supports the whole network.

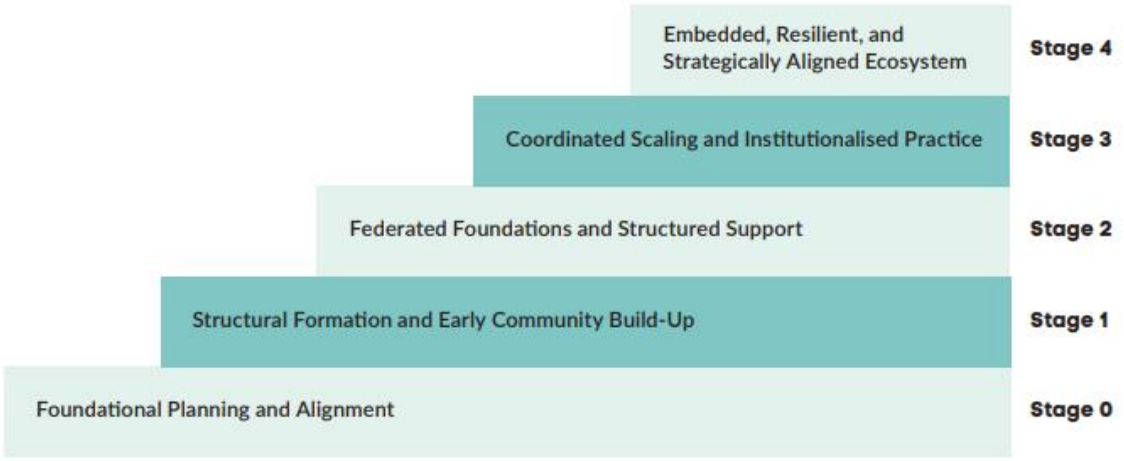

Figure 2: Five stage maturity model prescribing how the national support structure can evolve and mature in a coherent and systematic approach.

A stage-based model for practical, sequenced implementation

The development of a national, federated support structure for OSS requires a sequenced, capability-building approach. A staged maturity model is, therefore, defined, prescribing how Denmark can move from today's fragmented practices to a coherent, resilient ecosystem that supports national digital sovereignty.

Stage 0 – Foundational planning and alignment establishes the mandate and minimal structures needed to begin coordinated action. A National Government OSPO is set up within the Agency for Digital Government and staffed with OSS expertise and community trust as key requirements, an OSPO Network is formed across key actors, initial strategy work begins, and prototypes for essential guidelines and processes, as well as the national OSS catalogue and social code collaboration platform are launched.

Stage 1 – Structural formation and early community build-up focuses on validating early tools, processes, and support functions. A Regional Government OSPO is established, and OS2 is formalised as an Association-based OSPO responsible for scaling OSS support across municipalities. Procurement templates with sovereignty requirements are drafted and evaluated, intake and release processes are formalised, communities of practice emerge, stewardship pathways for OSS project archetypes are defined, and initial training builds basic competence across PSOs.

Stage 2 – Federated foundations and structured support matures support through revised processes and guidelines based on lessons learned, national funding programmes are launched, and communities of practice mature into national working groups supported by shared governance and maintenance cycles.

Stage 3 – Coordinated scaling and institutionalised practice formally embeds OSS considerations into procurement, compliance, and development routines. Reuse becomes standard practice, compliance processes and SBOM-based checks are widely adopted, and multi-year funding strengthens critical shared infrastructure.

Stage 4 – Embedded, resilient, and strategically aligned ecosystem completes the transition. Open-by-default becomes routine where appropriate, long-term stewardship and funding are stable, and Denmark actively contributes to European digital commons while maintaining a metrics-driven, sovereignty-aligned digital ecosystem.

(For further reading, see section 7.4)

Recommendations and guardrails to guide national action

OSS provides a strategic tool (among many) for countries, such as Denmark, to build digital autonomy and resilience. Yet it is important to stress that it is a tool, not a magic wand, and to use a tool correctly, one needs to learn how to use it. OSS in this context requires a culture and practice of collaboration, openness, and transparency, where change management, training, and advocacy are essential. Capabilities as such need to be organised and coordinated within a support structure that enables collective growth and learning, and action towards the vision of a more digitally sovereign future.

Although Denmark already benefits from strong forerunners and promising collaborations, these efforts remain fragmented, lacking scale and mandate. Nevertheless, they offer a valuable foundation and a strategic opportunity to advance toward greater digital sovereignty. Building on this reality, the report outlines the capabilities required and proposes pathways for organising them so that Denmark can progress from today's dispersed initiatives to a coherent, sustainable, and sovereignty-aligned digital ecosystem. The commissioning bodies are therefore strongly encouraged to adopt the proposed stage-based approach to systematically grow these capabilities over time.

The scope of this report has been limited to investigating how OSS can be supported on a national scale in Denmark and its public sector. Some consideration, though limited, has been given to using other open technologies that provide a complementary toolset to OSS, including open standards and open source AI. The academic and scientific contexts, civil society, as well as general linkage, policy and support for the industry have also received limited attention. Future work and investigation are strongly encouraged into how the public-sector support structure can extend and integrate with the wider society, considering open technologies at large as a lever for digital sovereignty, interoperability, and innovation.

Content

Abstract **2**
Executive summary **3**
Content **11**
General glossary **15**
Organisations glossary **16**
1 Introduction **19**
2 Related work **22**
2.1 What defines an OSPO? 22
2.2 Structures of an OSPO in the industry 22
2.3 Roles within an OSPO in the industry 24
2.4 Responsibilities of an OSPO in the industry 24
2.5 OSPOs from a policy perspective 25
2.6 OSPO archetypes 26
2.6.1 National Government OSPOs 26
2.6.2 Local Government OSPOs 27
2.6.3 Association-based OSPOs 27
2.6.4 Institution-centric OSPOs 27
2.6.5 Academic OSPOs 28
2.6.6 Organisations with OSPO-Like Support Functions 28
3 Research design **29**
3.1 Literature review 29
3.2 Interview survey of Danish context 29
3.3 Interviews with European reference OSPOs 30
3.4 Workshop for validation 30
4 Goals and policy incentives (RQ1) **31**
5 Barriers and challenges (RQ2) **34**
5.1 Strategic and leadership misalignment 34
5.2 Market power, procurement culture, and structural lock-In 35
5.3 Organisational and technical capabilities 35
5.4 User experience, productivity, and perceived operational risk 36
6 Capabilities required (RQ3) **37**
6.1 Capability to translate and shape open source policy and strategy 39
6.1.1 EU regulatory implementation and EU-level engagement 40
6.1.2 Engaging in European standardisation efforts 41
6.1.3 Strategic input and advisory support to policymakers 42
6.1.4 Institutional open source strategy development 42

6.1.5 Cross-government coordination and alignment with broader policy goals 43
6.2 Capability to design and operationalise policy instruments 45
6.2.1 Policy approaches: prescriptive and advisory models 46
6.2.2 Ownership models to enable sharing and reuse 47
6.2.3 Control mechanisms without ownership 47
6.2.4 Standardised requirements and contract templates 48
6.2.5 Procurement support and practitioner guidance 49
6.2.6 Decision support for open source release 50
6.2.7 Guidance for project initiation and community development 51
6.2.8 Sustainability and supply-chain Risk management 52
6.2.9 Policy considerations for open source AI 53
6.3 Capability to invest in, prioritise, and scale strategic open source alternatives 54
6.3.1 Strategic seed funding and impact demonstration 55
6.3.2 Maintenance funding of vital infrastructure 56
6.3.3 Prioritisation frameworks and migration pathways 57
6.3.4 Joint agreements and coordinated rollouts 59
6.3.5 Designing standards and reference implementations for sovereign digital infrastructure 59
6.3.6 Dual-channel adoption strategies..... 60
6.4 Capability to provide and coordinate shared open source collaboration infrastructure 61
6.4.1 Government social code collaboration platform 62
6.4.2 Government open source solution catalogue 63
6.5 Capability to manage open source licence selection and compliance 65
6.5.1 Curated licence lists and policy guidance..... 66
6.5.2 Embedded compliance in intake rocesses..... 66
6.5.3 SBOM-based compliance monitoring 66
6.5.4 Pre-release IP and licence verification 67
6.5.5 Periodic audits and software inventory management.....67
6.5.6 Procurement-integrated licence compliance.....67
6.5.7 Compliance considerations for AI-assisted code generation 68
6.6 Capability to steward public-sector open source projects 69
6.6.1 Association-based stewardship models..... 69
6.6.2 Supplier-led stewardship models 70
6.6.3 Government-internal stewardship models..... 70

6.6.4 State-owned service-provider stewardship models 71
6.7 Capability to measure, analyse, and follow up on open source activities 72
6.7.1 Demonstrating value and securing long-term support 73
6.7.2 Operational oversight and risk management 73
6.7.3 Platform, project, and service improvement 73
6.7.4 Sustainability and project health monitoring 74
6.7.5 Learning, capability-building, and needs identification 74
6.7.6 Feedback loops to strategy and policy 74
6.8 Capability to enable Inner Source collaboration 75
6.8.1 Inner Source for intra-governmental collaboration 75
6.8.2 Open-by-default as preferred development practice 76
6.8.3 Inner Source as an on-ramp to open practice 76
6.8.4 Social code collaboration platforms as Inner Source enablers 77
6.9 Capability to drive advocacy and build open source communities 78
6.9.1 Communities of practice 78
6.9.2 Multi-stakeholder advisory structures 79
6.9.3 Cross-government and cross-border collaboration 79
6.9.4 Advocacy for cultural and organisational change 80
6.10 Capability to provide training and build organisational competence 81
6.10.1 Training activities and delivery mechanisms 81
6.10.2 Role-specific training themes and target audiences 83
7 Organisation of and roles within the support structure (RQ4) 84
7.1 Key considerations for support structure 85
7.1.1 Build on what exists 85
7.1.2 Position the OSPO where mandate, authority, and feedback loops align 86
7.1.3 Distribute capabilities 87
7.1.4 Balance and connect policy-shaping with technology enablement 87
7.1.5 Enable both inward- and outward-facing support 88
7.1.6 Embed communication, storytelling, and change management 89
7.1.7 Enable sustainable stewardship of public-sector OSS 89
7.1.8 Create multi-level coordination mechanism 90
7.1.9 Treat funding as a strategic design parameter 90
7.1.10 Reduce bureaucracy through reusable artefacts and automation 91
7.1.11 Ensuring the right expertise and community trust in OSPO staffing 91
7.2 Architectural options for a multilevel support structure 93
7.2.1 Centralised model 93

7.2.2 Decentralised model 94
7.2.3 Federated model 95
7.3 Proposed Danish OSPO-based support structure 96
7.3.1 National Government OSPO – aggregated support on the national level and cross-government coordination 97
7.3.2 Regional Government OSPO – aggregated support and coordination on the regional level 99
7.3.3 Association-based OSPO – aggregated support and coordination on the local government level 99
7.3.4 Local Government OSPOs – local and focused support and community enabler 100
7.3.5 Institution-centric OSPOs – internally focused support for resourceful organisations 100
7.3.6 Supporting national functions 101
7.3.7 National OSPO Network 102
7.4 Maturity model and evolution path 103
7.4.1 Stage 0 – Foundational planning and strategic alignment 105
7.4.2 Stage 1 – Structural formation and early community build-up 106
7.4.3 Stage 2 – Federated foundations and structured support 107
7.4.4 Stage 4 – Embedded, resilient, and strategically aligned ecosystem 109
8 Conclusions and future outlook 110
9 References 111
10 Annex A – Interviewee and workshop participant demographics 118
11 Annex B – Interview questionnaire 120
11.1 Introduction and background 120
11.2 Strategic goals and vision (RQ1) 120
11.3 Barriers and challenges (RQ2) 120
11.4 Capabilities required (RQ3) 120
11.5 Existing actors and frameworks (RQ4) 121
11.6 Realization through OSPOs (RQ5) 121
11.7 Reflections and outlook 121

General glossary

General constructs and abbreviations used throughout the report.

- CRA – Cyber Resilience Act
  - EU regulation setting cybersecurity and resilience requirements for digital products and services.
- Digital commons
  - Shared, openly governed digital resources (software, data, standards) reusable by many actors.
- Digital public infrastructure
  - Shared foundational digital systems (e.g., identity, payments, data exchange) supporting multiple public services.
- Digital sovereignty
  - The ability of a state or public sector to control and govern its own digital infrastructure, data, and technologies.
- IEA – Interoperable Europe Act
  - EU regulation promoting cross-border interoperability of public-sector digital systems and data.
- Interoperability
  - The ability of different systems and organisations to exchange and use data seamlessly.
- Open standard
  - A publicly documented standard that can be implemented without restrictive conditions or licensing.
- OSS – Open Source Software
  - Software whose source code is openly available for use, modification, and redistribution.
- OSPO – Open Source Program Office
  - Organisational unit that coordinates OSS strategy, governance, and contributions.
- PSO – Public-Sector Organisation
  - Any governmental or publicly funded body delivering public services or digital infrastructure.
- Vendor lock-in
  - A situation where switching suppliers or technologies becomes difficult or costly.

Organisations glossary

A sample of organisations highlighted throughout the report, both Danish and international.

International:

- Adullact
  - French public-sector association stewarding and promoting collaborative open-source solutions.
- Cabinet Office (UK)
  - Home of the Government Digital Service, illustrating the value of central placement for digital governance.
- CEN – European Committee for Standardization
  - Develops voluntary European standards across non-electrotechnical domains to support safety, interoperability, and harmonised practices.
- CENELEC – European Committee for Electrotechnical Standardization
  - Produces European standards for electrical and electronic technologies, ensuring safety, reliability, and market consistency.
- Codeberg e.V.
  - Non-profit hosting Forgejo, a federated, community-governed alternative to proprietary Git forges.
- DIGG – Swedish Agency for Digital Government (Myndigheten för digital förvaltning)
  - Swedish national body proposing OSS collaboration platforms and OSPO-aligned support models.
- DINUM – French Interministerial Digital Directorate (Direction interministérielle du numérique)
  - Central French government body providing national OSS governance, platforms, and catalogue.
- Dutch National Government OSPO (I-Interim Rijk / BZK)
  - Interministerial unit coordinating national OSS policy, catalogues, and ministry-wide collaboration.
- EDIC-DC – European Digital Infrastructure Consortium for Digital Commons
  - EU-level consortium coordinating development and governance of shared digital commons infrastructure.
- ETSI – European Telecommunications Standards Institute
  - Creates globally recognised standards for ICT, including telecommunications, radio systems, and internet technologies, enabling interoperable digital infrastructures.
- European Commission OSPO Network
  - EU network connecting public-sector OSPOs to share best practices and align catalogues.
- European Standardisation Organisations (ESOs)
  - Collective term for CEN, CENELEC, and ETSI, the three EU-recognised bodies responsible for developing European standards that support legislation, interoperability, and the functioning of the Single Market.

- German Open Source Business Alliance (OSBA)
    - Industry association offering OSS procurement criteria and frameworks for public administration.
- Government Digital Service (GDS)
    - UK central digital institution known for delivery-led policy, open standards, and “open by default” practices.
- iMio
    - Walloon public digital service provider offering open digital tools and shared municipal services.
- Open Cities
    - Czech municipal network stewarding and governing OSS solutions similar to OS2 and VNG.
- OpenForum Europe
    - European policy think-tank for open technologies, including OSPOs and strategic autonomy.
- Open Regulatory Compliance Working Group (ORC WG)
    - Eclipse Foundation working group developing open specifications to help OSS communities and industry comply with emerging regulations, including the EU Cyber Resilience Act, while maintaining sustainable OSS use in the software supply chain.
- OSPO Alliance
    - European initiative providing maturity models, best practices, and guidance for public-sector OSPOs.
- OperatorICT
    - Prague’s public operator providing open source-based municipal digital services.
- pagoPA (pagoPA S.p.A.)
    - Italian state-owned company operating national digital platforms and OSS-based public services.
- Sambruk
    - Swedish municipal OSS network collaborating on shared digital services and reuse.
- Schleswig-Holstein State OSPO (Land Schleswig-Holstein / WTSH DigitalHub.SH)
    - Regional OSPO demonstrating effective dual-level support, funding schemes, and communication-driven transformation.
- Sovereign Tech Agency (Germany)
    - Federal programme funding maintenance and security for critical OSS infrastructure used across government.
- VNG – Association of Dutch Municipalities (Vereniging van Nederlandse Gemeenten)
    - Dutch municipal association acting as OSS steward and supplier-neutral governance body.
- WTSH GmbH – DigitalHub.SH
    - Regional innovation hub hosting Schleswig-Holstein’s OSPO and coordinating cross-government collaboration.

Danish:

- Agency for Digital Government (Digitaliseringsstyrelsen)
    - National body setting digital-government architecture, standards, and OSS guidance.
- Agency for Governmental IT Services (Statens IT)
    - State-owned IT operator delivering shared digital infrastructure and potential steward for OSS.
- Agency for Governmental IT Services IT Council (Statens IT-råd)
    - Central advisory body reviewing and risk-assessing major state IT projects.
- Aarhus Municipality (Aarhus Kommune)
    - Front-running Danish municipality with strong OSS adoption, migration efforts, and contribution practices.
- Danish Court Administration (Domstolsstyrelsen)
    - National authority responsible for the administration, organisation, and digital support of the Danish court system.
- Danish Road Traffic Authority (Færdselsstyrelsen)
    - National agency overseeing vehicle regulation, driver licensing, and digital services related to road traffic safety and compliance.
- DBC Digital
    - National public digital actor supporting shared solutions and sector-wide services.
- KOMBIT
    - Public-sector enterprise coordinating common municipal IT solutions and reuse frameworks.
- Local Governments Denmark (KL)
    - Umbrella organisation for municipalities, central for policy alignment, procurement support, and OSPO collaboration.
- OS2
    - Danish association-based OSPO stewarding municipal OSS through mature governance frameworks, and procurement models.
- SKI – National and Municipal Procurement Service (Statens og Kommunernes Indkøbsservice)
    - Procurement agency managing framework agreements where OSS-relevant clauses and scoring can be embedded.
- Statens Indkøbsprogram (Økonomistyrelsen)
    - State procurement programme enabling framework updates for OSS ownership, reuse, and exit clauses.

1 Introduction

While European societies are becoming ever more interconnected, their ability to maintain agency over critical digital services and infrastructures is decreasing (Folketinget, 2025). Historical under-investments and an accumulation of dependencies and lock-in to incumbent vendors across the hardware, cloud and digital service layers are contributing to asymmetries in market power and limitations in choice and freedom for buyers and consumers (European Parliament, 2026). Escalating licensing costs has pushed sense of urgency to a tipping point (PwC, 2019), with recent regulatory and geopolitical developments adding on top with a new set of critical risks (Di Marco et al., 2025; Edler et al., 2023) where data, digital infrastructure and supply chains can be used as leverage in policy and trade, and even become a national security concern (Bellanova et al., 2022).

European leaders are calling for "a new form of European independence" (von der Leyen, 2026), in which Europe and its nation-states must recognise and treat digital sovereignty as a key priority (European Parliament, 2026). Digital sovereignty, in this context, can be understood as Europe's "capacity to design, develop and scale up digital technologies needed for the competitiveness of the economy, the welfare of its citizens and the EU's open strategic autonomy in a globalised world" (European Parliament, 2026).

For Denmark, digital sovereignty is accordingly seen as a major concern and priority (Folketinget, 2025), with calls for increased promotion and growth of choice and competition, as well as investments into pilots to grow experience and capabilities (Regeringen, KL, & Danske Regioner, 2025). Recent analysis further strengthens concerns regarding the lack of control, governance, and transparency over data and software, as well as the cybersecurity and geopolitical risks that accompany them (PA Consulting, 2026). The same analysis further centres attention to Open Source Software (OSS) as a key tool for enabling and promoting digital sovereignty, something also echoed across research (Blind et al., 2021; Edler et al., 2023), ministerial declarations(European Commission, 2017a, 2020a, 2022), and more recently in EU's coming sovereignty package, including an EU-level OSS strategy, and the Cloud and AI Development Act (European Commission, 2026).

OSS, essentially, provides a reusable type of building block present in 95% of digital infrastructure across industry and society. By design, OSS enables its users to exercise control over studying, using, modifying, and sharing the software according to their own agendas (Blind et al., 2021). However, to build autonomy and leverage the technological opportunities OSS brings, the public sector needs to develop the necessary capabilities (Digitaliseringsstyrelsen, 2025) and address the several challenges that historically persist (Linåker & Muto, 2024). A consistent outsourcing of technical capabilities through consultancies and vendors (Marco-Simó & Pastor-Collado, 2020) has limited the know-how in software engineering and practice (Borg et al., 2018), and how these can be considered in the procurement and acquisition of software solutions (Lundell et al., 2021). Conservative and risk-averse procurement culture, with preference of a status-quo, is another critical challenge, embedding the public sector into a state of comfort (Persson & Linåker, 2024). Short-sighted planning,

along with a lack of political support and insight, further complicate the situation (Linåker et al., 2025a).

Adoption of OSS at a strategic level (i.e., as a means of achieving overarching strategic goals, such as digital sovereignty) essentially requires organisational and cultural change, as well as support structures to advise and execute the strategy (Linåker & Muto, 2024). In response, an organisational construct referred to as Open Source Program Offices (OSPOs) has emerged, originally from the software industry shortly after OSS was introduced (Ruff, 2022). The OSPOs provide centres of competency and support for their respective organisations (European Commission, 2020b), helping to accelerate organisational readiness and grow capabilities to adopt, develop and collaborate on OSS (Digitaliseringsstyrelsen, 2025). Essentially, the OSPOs act as change agents in their respective contexts, working to onramp cultural mindsets and ways of working into the open innovation paradigm (Linåker et al., 2024).

Public-sector OSPOs are increasingly emerging across Europe to address growing needs for digital sovereignty, while also taking advantage of the potential innovation and economic upside that OSS offers (Linåker & Muto, 2024). The Centre for Digital Sovereignty (ZenDIS) in Germany, and the regional OSPO of Schleswig-Holstein are two prominent examples (PA Consulting, 2026), while several others have been studied across national, regional and local levels of government (Linåker et al., 2024), including single governments and Public Sector Organisations (PSOs), as well as association-based OSPO structures (Digitaliseringsstyrelsen, 2025). In cases where governments lack the resources and will altogether, civil society has been found to provide complementary support structures. Academic OSPOs have also been reported across Institutes for Research and Higher Education.

In this report, commissioned by Local Governments Denmark (KL) and the Danish Agency of Digital Government (Digitaliseringsstyrelsen), we consider the specific context of Denmark, and how its governments and PSOs can grow the capabilities necessary to enable sharing and reuse of OSS, grow a strategic autonomy (Edler et al., 2023), and exploit the opportunities OSS provides (Blind et al., 2021). Specifically, we build on the recommendation from the analysis of digital sovereignty in the Danish public sector, commissioned by the Danish Agency of Digital Government (Digitaliseringsstyrelsen) and Local Governments Denmark (KL), which proposes establishing a national centre for digital sovereignty and innovation (PA Consulting, 2026). Using the OSPO construct (Digitaliseringsstyrelsen, 2025), we aim to propose a design and strategy for the consideration and implementation of public-sector OSPOs that can support incentives and policy goals in the context of digital sovereignty in Denmark.

Through this study, we ask and address the following questions:

- RQ1: How are strategic goals and vision in terms of digital sovereignty and potential opportunities of cross-government collaboration, sharing and reuse of OSS solutions characterised among Danish PSOs?
- RQ2: What are the central barriers for cross-government collaboration, sharing and reuse of OSS solutions among Danish PSOs?
- RQ3: What capabilities are required for cross-government collaboration, sharing and reuse of OSS solutions among Danish PSOs?

- RQ4: How can the identified capabilities be enabled and realised through public-sector OSPOs in Denmark?

Based on research findings, the report synthesises and presents recommendations and a plan for activities and frameworks to initiate the desired cross-government collaboration by establishing public-sector OSPOs in Denmark.

To address the challenges, we adopt a qualitative yet triangulating research approach. First, by consulting public policy and scientific literature in the context of Denmark and internationally. Second, through semi-structured interviews with practitioners from stakeholders in the Danish public sector and wider OSS ecosystem. Third, through semi-structured interviews with reference cases of public-sector OSPOs across Europe. Fourth, through several focus groups to validate and enrich findings. Findings are iteratively synthesised using thematic analysis and validated through continuous member-checking with the sources and peer-debriefing with representatives of the commissioning bodies of this study.

The remainder of this report is structured as follows. We begin by outlining relevant and related work identified in our literature review. We then present the research design and methodological approach underpinning the study. This is followed by our empirical findings, organised according to the defined research questions. We next discuss these findings in relation to prior work, reflect on the study's validity, and develop recommendations, together with a practical plan for how public-sector OSPOs can be realised in Denmark. Finally, we conclude by summarising key insights and identifying avenues for further work in policy, practice and research.

2 Related work

2.1 What defines an OSPO?

The concept of Open Source Programme Offices as a construct originates from industry at the beginning of the 2000s among larger software-intensive companies such as Sun Microsystems, Hewlett-Packard, Intel, and Google (Ruff, 2022; Phipps, 2021). Since then, the concept has grown and matured as several organisations and industries, including those outside the software industry, have adopted the construct (The TODO Group, 2022b).

With the growth of OSPOs, so has the definition and views of what an OSPO is. The TODO Group, an industry network, describes an OSPO as a "centre of competency for an organisation's OSS operations and structure" which may include responsibilities such as designing and facilitating processes for selection and intake of OSS, compliance and auditing, contributions and community engagement, as well as training for an organisation's different stakeholders (The TODO Group, 2022a). The OSPO Alliance (a joint initiative by for example, OW2, Eclipse Foundation, OpenForum Europe, and Foundation for Public Code) considers an OSPO as "a cross-functional team to help define and steer an organisation's OSS management strategy and organisational readiness" (OSPO Alliance, 2021). Both networks agree that there is no "one-size-fits-all". Rather, its tasks and responsibilities will vary in line with the organisation's overarching goals, strategies, and views on OSS.

From a public-sector perspective, the concept is still emerging, and commonly under different naming conventions, although with similar meanings. OpenForum Europe, for example, considers it as "an institutional organisational construct that supports and accelerates the consumption, creation, and application of Open Source software" (OpenForum Europe, 2022). Specifically, they highlight the focus on "working strategically to achieve the policy objectives of the institution that intersect with Open Source", which contrasts with the business perspective in industry OSPOs. However, from a general perspective, the focus remains on enabling OSS as a tool for creating value aligned with the goals of the focal organisation, whether public or private.

OSPO++, a network and community of collaborative OSPOs, universities, governments, and civic institutions, accordingly, looks at the construct from a public-sector perspective, highlighting both municipal, government, and university settings. They consider how the public context can bring other organisational structures, incentives, and levels of bureaucracy than the private context (Dillon & Litthauer, 2021). The common trend of outsourcing and acquiring technical capabilities (Mikalsen & Farshchian, 2020), along with otherwise symptomatic short-term planning and risk-averse culture (Alanne et al., 2015), further adds nuance that might affect how OSPOs in PSOs take shape.

2.2 Structures of an OSPO in the industry

The structure and organisational location of an OSPO vary depending on its goals and purpose. Haddad (2020) reports on five examples of how an OSPO can be set up in an

industrial setting (see Table 1). The examples vary in terms of their internal sponsor, budget, staffing, which entities they support, and the size of the organisation they are suitable for, as presented in the table below.

Table 1: Overview of different OSPO structures observed in the industry setting. Adopted from Haddad (2020).

	Sponsor	***Supporting entities***	***Budget***	***Staffing***	***Organisation***
OSPO within R&D org.	Executive mgmt for R&D	R&D division and product departments	Dedicated	Head of open source + dedicated staff	Large organisations with single product division
Corporate-level OSPO with supporting division level functions	Executive mgmt	Multiple divisions	Dedicated	Head of open source + dedicated staff	Large organisations with multiple product division
Virtual OSPO	CTOs office or head of engineering	Main organisation	Partial funding across different functions	Head of OSS + part time distributed team	Small and medium-sized organisations
No official OSPO	Executive mgmt	Main organisation	Partial funding across different functions	Part time distributed team	Small organisations
OSPO as part of CTO office or Engineering	CTOs office or head of engineering	Main organisation	Dedicated	Head of open source + dedicated staff	Medium-sized organisations

The first example puts the OSPO within the R&D organisation with direct sponsorship and reporting to executive management. This setup isolates the OSPO from product departments, enabling it to execute on a general OSS strategy not limited by specific product strategies. More freedom to collaborate with external parties is also given.

The second, yet similar, example places the OSPO at the corporate level, with support functions in each division when multiple product divisions are present. The support functions help adapt and implement OSS strategies, policies, and processes for each

division's context. In a third example, a virtual OSPO, there is typically a main responsible head of OSS, but without a fully dedicated team. Individuals from different functions instead work part-time on related tasks coordinated by the head of OSS.

In a fourth example, there is no official OSPO present. Rather, the associated tasks are spread out over multiple individuals, a suitable option for smaller organisations. In the fifth and final example, the OSPO is positioned as a part of the CTO office or the engineering organisation, suitable for medium-sized organisations (Haddad, 2020).

2.3 Roles within an OSPO in the industry

As with the structure and organisational location, the staffing of the OSPO depends on its goals and purpose. Haddad (2020) differentiates between five different roles, although highlighting that they do not necessarily need to be divided among different individuals. Rather, they can be shared or aggregated, depending on the OSPO's structure. Roles include:

- A head of OSS is responsible for the design and execution of the organisation's OSS strategy. The head also manages the reporting and follow-up of the strategy's progress to the OSPO's sponsor.
- A software architect is proposed with responsibility for high-level technical decisions related to OSS and the organisation's various products and platforms.
- A technical evangelist is proposed to support and promote OSS contributions, engagement, and culture across the organisations and externally in relevant communities and foundations.
- A compliance engineer is proposed to oversee and maintain compliance related to the organisation's OSS intake.
- A legal counsel is proposed who is knowledgeable in OSS licensing.

In their classification, the TODO Group differentiates between roles focusing on governance, project management, licensing, security, community engagement, developer education, individual contributors, and OSS advice (TODO, 2024).

2.4 Responsibilities of an OSPO in the industry

The TODO Group has defined a set of responsibilities typically maintained by OSPOs based on industry practice and an underpinning report by Haddad (2020). Exactly which responsibilities an OSPO maintains depends on its purpose. Further, as responsibilities originate from state-of-practice in an industry context, not all may be relevant or correctly defined for the public sector. Still, they provide a point of departure when investigating what responsibilities public-sector OSPOs take on. Below, we briefly summarise and describe an OSPO's responsibilities primarily based on the work by Haddad (2020):

- **Develop and Execute OSS Strategy** - An OSPO is responsible for setting and implementing an organisation's long-term OSS strategy. This involves defining goals related to OSS consumption, participation, contribution, and leadership, depending on the organisation's maturity and objectives.

- **Oversee OSS Compliance** - OSPOs manage compliance with OSS licenses to mitigate legal risks. This includes designing processes and policies to ensure obligations are met, protecting intellectual property, and managing potential infringements.
- **Establish and Improve OSS Policies and Processes** - OSPOs develop policies that guide the organisation's OSS activities, including consumption, contribution, and business decisions. They also create processes for project creation, code release, communication, and training.
- **Prioritise and Drive OSS Upstream Development** - Organisations must prioritise which OSS projects to invest in. OSPOs help identify critical projects and establish strategies for community engagement, ensuring alignment with the overarching OSS strategy.
- **Collaborate with OSS Organisations** - OSPOs engage with relevant OSS organisations and foundations to align with business goals and influence key technologies. This collaboration can provide strategic advantages and influence within the OSS community.
- **Track Performance Metrics** - OSPOs measure the impact of OSS activities through performance metrics that align with business goals. This requires expertise in both metric design and operationalisation to support strategic objectives.
- **Implement Inner Source Practices** - Inner Source involves using OSS development practices internally to improve collaboration. OSPOs facilitate this by providing infrastructure, education, and support for cross-functional teamwork.
- **Grow and Retain OSS Talent Inside the Organisation** - Training programs are essential for developing internal OSS capabilities. OSPOs offer workshops, mentorships, and ambassador programs to nurture talent and integrate OSS contributions into performance reviews.
- **Provide Advice and Support on OSS** - OSPOs advise stakeholders on leveraging OSS in business strategies, evaluating technologies, setting community engagement goals, and ensuring compliance in various contexts such as mergers or outsourced development.
- **Manage Open Source IT Infrastructure** - OSPOs manage the infrastructure necessary for engaging with OSS projects and supporting Inner Source initiatives. This includes tools for compliance tracking, vulnerability scanning, and contribution monitoring.

2.5 OSPOs from a policy perspective

A report from OpenForum Europe (2022a) argues that the emergence of OSPOs results from the acknowledged need to increase OSS competence across different parts of public-sector administration. OpenForum Europe, looking at trends from a managerial perspective, finds that the motivations for building OSPOs in the public sector are diverse, but generally observes a growing acknowledgement that OSS is essential to the public sector and that it is already used in everything from IT infrastructure to e-government services.

Herpig (2023) specifically highlights the criticality of cybersecurity and the need for establishing a Cyber Security OSPO, a recommendation also highlighted by the US Cybersecurity and Infrastructure Security Agency's (CISA's) Open Source Software Security Roadmap (CISA, 2023). Main tasks include monitoring the national OSS supply chain, educating on OSS security practices, advising policymakers, supporting OSS infrastructure development, and interfacing with the broader OSS ecosystem. These recommendations align with broader changes in the political environment for OSS and OSPOs, where there is an increasing emphasis on software supply chain security and on the ability to make technical sourcing and design decisions based on local needs, values, and laws (OpenForum Europe, 2022b).

From a more general perspective, both OpenForum Europe (2022a) and the Linux Foundation (2023) emphasise that sharing and reuse of software between PSOs hold the greatest promise for benefits. Economic growth (Blind et al., 2022), increased competitiveness and entrepreneurial growth (Nagle, 2023; Wright, 2023), and long-term interoperability (European Commission, 2017b) are among these benefits, as are targets for potential policy interventions.

Several reports, therefore, also provide policy recommendations, including the establishment of OSPOs that look beyond the specific topic of cybersecurity (CISA, 2023; Herpig, 2023). The Mission Bothorel (2021) report proposed the establishment of an OSPO in France, which was subsequently instantiated as the Free Software Unit at the French Interministerial Digital Directorate (Direction interministérielle du Numérique - La DINUM). Similar proposals have been laid forward in the US context (Nagle, 2022), proposing a federal government OSPO aimed at coordinating OSS policies with other public-sector OSPOs, as well as overseeing and advising in the general implementation of OSS policy interventions, and interfacing with the general OSS ecosystem and other OSPOs on the international level.

2.6 OSPO archetypes

In their study of OSPOs in the European public sector, Linåker et al. (2024) identified six main OSPO archetypes across the 12 cases they surveyed. While not complete, the archetypes represent patterns of structure and activities taken on by OSPOs across different parts of the public sector. Below, the archetypes are summarized in a high-level overview.

2.6.1 National Government OSPOs

National Government OSPOs typically act as central coordinators for OSS adoption across an entire country's public sector, commonly situated within ministries or national digital-government bodies. Their mandate revolves around operationalising high-level digital-sovereignty and open technology policies by translating political ambition into actionable processes, guidelines, and shared infrastructures. They develop and maintain national catalogues, social code collaboration platforms, and legal or procurement frameworks that position OSS as a systematic option in public software acquisition and development. Where resources allow, these OSPOs may also steward strategically important OSS applications that underpin sovereign digital capabilities, exemplified by national workspaces or cybersecurity tooling. Their role

extends to building communities of practice, fostering cross-government knowledge exchange, and engaging with the broader OSS ecosystem to ensure alignment between public needs and upstream developments. While capacity varies across countries, these OSPOs share a unifying ambition: to grow institutional competence across all levels of government and embed OSS as a foundational element of national digital governance.

2.6.2 Local Government OSPOs

Local Government OSPOs operate within municipalities, cities, or regions and are tightly coupled to the digital transformation needs of their local administrations. These OSPOs frequently combine strategic support with hands-on software development, reflecting the practical and immediate needs of municipal service delivery. While formal OSS strategies may be absent in some local governments, OSPO efforts are often anchored in broader innovation agendas or mandated by national policy requirements. Local OSPOs commonly steward key municipal platforms, such as e-service portals or modular website frameworks, and actively publish their work as OSS, both to enhance transparency and to enable other municipalities to reuse and adapt their solutions. Their responsibilities encompass procurement support, licensing decisions, and maintenance of software inventories, while their collaborations often extend to neighbouring cities or international peers to share practices and jointly strengthen local open-technology ecosystems. Despite their smaller size, these OSPOs are crucial actors in demonstrating tangible OSS impact at the front lines of public service delivery.

2.6.3 Association-based OSPOs

Association-based OSPOs are collective, member-driven entities that provide municipalities and other PSOs with a neutral organisational framework for jointly governing and developing OSS solutions. They enable public bodies, which are often resource-constrained at the local level, to pool expertise, share costs, and collaborate on digital tools addressing common policy and service needs. These organisations take on community-management functions, maintain governance structures for OSS projects, and support procurement, vendor interaction, compliance, and sustainability planning. Their project portfolios frequently span multiple municipalities and evolve into de facto shared digital infrastructures within the national context. Association-based OSPOs also promote cross-jurisdictional collaboration, both domestically and internationally, and serve as important intermediaries between PSOs and market suppliers. By providing long-term stewardship in a politically neutral setting, they create stable conditions for public-sector OSS development, ensuring continuity, trust, and scalability across participating members.

2.6.4 Institution-centric OSPOs

Institution-centric OSPOs are embedded within large public institutions, such as national agencies, tax authorities, or EU bodies, and focus on strengthening OSS adoption and collaboration within the organisation itself. Their responsibilities centre on shaping internal OSS strategies, enabling safe and efficient OSS intake, and supporting contributions and releases through lightweight compliance and approval processes that balance autonomy with organisational risk management. These OSPOs serve as internal connectors, aligning developers, legal experts, security officers, and

managers around shared practices for open development. They provide internal infrastructure, such as code-hosting platforms or testing environments, and facilitate relationships with external OSS communities or networks to ensure that institutional work remains interoperable and outward-looking. Although their remit is narrower than national OSPOs, they play a crucial role in cultivating internal awareness, trust, and competence, often acting as boundary-spanning units that embed open collaboration practices into the organisation's daily operations.

2.6.5 Academic OSPOs

Academic OSPOs sit within universities or research institutes and focus on supporting researchers in developing, managing, and disseminating software outputs as OSS while balancing intellectual-property obligations, funding conditions, and open-science principles. These OSPOs operate at the intersection of research practice and institutional policy, advising on licensing, commercialisation pathways, and opportunities for spin-outs. They also provide practical infrastructure and training for researchers, fostering competencies in collaborative development, community engagement, and software publication. Academic OSPOs frequently serve as internal champions for open science, promoting transparency and reproducibility across research domains. By participating in national and international networks, they facilitate knowledge exchange and amplify the societal value of publicly funded research through reusable, openly governed software artefacts. Their role is both educational and strategic, helping institutions integrate OSS practices into broader research-impact and innovation agendas.

2.6.6 Organisations with OSPO-Like Support Functions

Organisations with OSPO-like support functions, exemplified by entities such as Code for Romania, operate independently of formal public-sector structures but exist to strengthen OSS-based digital capabilities across civil society and government. These organisations design, develop, and maintain OSS solutions addressing critical societal needs, often stepping in where PSOs lack capacity, expertise, or flexibility to build solutions themselves. Their work is deeply user-centred and mission-driven, covering domains such as citizen engagement, social services, emergency response, and public-sector digital infrastructure. They contribute upstream to external OSS projects, implement rigorous development and documentation practices, and use metrics extensively to validate assumptions and monitor performance. Although not formal advocates, they actively educate and support policymakers and PSOs, demonstrating value through working systems rather than policy lobbying. These organisations exemplify how civil-society initiatives can accelerate and complement public-sector digital transformation, especially in contexts where institutional OSPO structures are nascent or absent.

3 Research design

We have structured our research in four phases. First, by surveying relevant literature; second, through semi-structured interviews with stakeholders from the Danish public sector and the OSS ecosystem; third, through semi-structured interviews with reference cases of public-sector OSPOs across Europe; fourth, through validation-focused workshops with interviewees, additional experts, and decision-makers. Below, we describe these phases in further detail.

3.1 Literature review

To gain an initial, contextual understanding of Denmark in relation to the specific research questions, both public policy, practice, and the scientific literature were consulted. Earlier work (Linåker & Muto, 2024; Linåker & Nummelin Carlberg, 2024) was used as a starting point for the review. Both public and scientific databases are used. Representatives from the commissioning bodies, as well as PSOs, were consulted throughout the research and were also asked to propose relevant literature for consideration in the review.

3.2 Interview survey of Danish context

To gain an in-depth understanding of the problem context, 15 semi-structured interviews were conducted with representatives from Danish PSOs and the wider national OSS ecosystem (see Annex A). Purposive sampling was used to obtain representation from relevant stakeholder categories, including policymakers and practitioners within PSOs at national, regional, and local government levels. Relevant unions and industry associations, and academic institutions were also considered.

Initial sampling was guided by earlier work (Linåker & Muto, 2024) and by input from the commissioning bodies of the study, who possess subject-matter and contextual expertise. Additional interviewees were identified through snowball recommendations coming from the initial sample.

A questionnaire was constructed based on the defined research questions and further refined based on the literature surveyed in the previous step (see Annex B). Interviews lasted about 60 minutes and were conducted either online or in person, depending on the availability of the interviewees and the researcher. Regardless, all interviews were recorded and transcribed using local and offline Large Language Models. Transcripts were analysed using thematic analysis and complemented by interview notes. Findings were accordingly iteratively analysed and synthesised to inform the following interviews, maintaining a flexible research design. The recommendations and plan for the design and implementation of public-sector OSPOs evolved continuously.

3.3 Interviews with European reference OSPOs

The interviews focused on the Danish public sector and OSS ecosystem, providing contextual and in-depth knowledge across RQ1-4. However, additional design knowledge was required to materialise the previously acquired knowledge related to RQ4 and to identify how identified capabilities can be enabled and realised through public-sector OSPOs in Denmark. Accordingly, several reference cases were selected through purposive sampling, with consideration of public-sector OSPO archetypes identified in earlier work (Linåker et al., 2023). Interviewees are listed in Annex A. The data collection and analysis approach was similar to that of the previous interview survey of the Danish context.

3.4 Workshop for validation

Workshops were facilitated on three occasions throughout the research process in parallel with the interview surveys. The goal was to validate and enrich synthesised findings in iterations to inform the research process.

The first two workshops included representatives from the commissioning bodies of this study, as well as a wider set of stakeholders from various stakeholders who are all part of a working group overseeing the practice and support for sharing and reuse of OSS across Danish PSOs. In the third workshop, interviewees and representatives from the wider OSS ecosystem in Denmark were invited to gain a broader view of the synthesised findings.

Each workshop centred around a selected set of propositions from the findings at the time of the research. Workshops were recorded and analysed retrospectively, supplemented by notes and data from the digital collaborative tool used for surveying participants. Findings fed into the analysis process of the interviews.

4 Goals and policy incentives (RQ1)

Summary:

Interviews point to a consistent rationale for leveraging OSS in Danish public administration, with a shift from generic vendor independence toward a broader sovereignty agenda. More specifically:

- Vendor independence and organisational autonomy remain the immediate aims, keeping the option to switch, adapt and operate systems without lock-in.
- Digital sovereignty has become a key policy incentive, linking technological control to jurisdiction, credible exit options and responsible data governance in a changing geopolitical context.
- Interoperability is treated as an essential enabler for digital sovereignty, with open standards and OSS enabling data exchange, service integration and cross-government reuse, including cross-border collaboration.
- Cost and efficiency continue to motivate adoption, as reuse and shared development reduce duplication, lower operating expenses and increase competition while supporting domestic and European supplier capacity, and by extension the digital sovereignty.

Below we describe the instruments and practices that translate these goals into procurement, development and governance.

Gaining control over IT beyond third-party providers is a main incentive for using OSS, as iterated across many of the interviews. There is a common understanding that it should be easy for PSOs to move their IT between vendors and switch out solutions based on their own preference and requirements.

The architectural principles, authored by the Agency for Digital Government (2022c), also emphasise that PSOs should avoid becoming dependent on any vendor or proprietary technology. Similar encouragement is also provided on the municipal level in corresponding principles from the Association of Municipalities (Kommunernes Landsforening, n.d.). Open standards and sustainable OSS solutions should be considered and used to the extent possible. The choice between OSS and proprietary technology should, however, be based on what delivers the best value for the needs at hand. The national principles from 2014 further describe how OSS can improve competitiveness among software vendors and enable sovereignty and control over how the software is used, developed, and shared (Digitaliseringsstyrelsen, 2014).

Digital sovereignty is commonly used as a construct to consider vendor lock-in in the context of geopolitical risk and is highlighted as a topic of wide urgency for Denmark, given recent geopolitical events, e.g., in the relationship between Denmark and the US. China is, however, also highlighted as a concern, citing how Huawei was blocked from

participating in the telco rollout due to digital sovereignty concerns. There is reported interest from policy and decision-makers in the origin of the technology underpinning various digital services, whether developed by, e.g., US or Chinese firms or by European firms.

One interviewee refers to sovereignty as the control over the digital representation of society and its institutions, where OSS is one tool among many. The selection and use of cloud providers that align with and comply with European data protection legislation are considered critical. One of the regional governments has, e.g., established its own cloud principles to promote conscious and safe use of cloud service.

The pragmatic, multi-layered approach to increased control is iterated at the local level, e.g., through the City of Aarhus. The city established its first process and strategy for the adoption and consideration of OSS in the acquisition process in 2011 through a local government decision, later enforced through the city's official OSS policy (Aarhus Kommune, 2014). The policy highlights that it is not a goal in itself. Instead, it is viewed as a means of achieving their overarching goals of adopting software based on open standards, avoiding recurring licensing fees, and avoiding lock-in to vendors and proprietary technologies.

A key requirement for enabling sovereignty, and a closely linked incentive, is that of *interoperability* for ensuring seamless and connected public digital services and data sharing nationally and cross-border. Solutions based on OSS typically follow open standards, provide reference implementations, and can be tailored to enable interoperable solutions. The Interoperable Europe Act further pushes for the release of interoperable solutions as OSS to enable cross-border sharing and reuse, to enable shared and integrated public digital services, e.g., for personal identification or payment systems.

The Agency for Digital Government's guidelines further highlight the need for flexible yet interoperable solutions that can be reused and modified to meet current needs. The importance of reuse is also echoed in a set of earlier-released principles on OSS use in the public sector, which note that taxpayers should not need to fund the acquisition of software solutions multiple times (Digitaliseringsstyrelsen, 2014).

Several interviewees also report cost savings and the principle of not having to buy the same system over and over again, since its development has already been funded by public money. While profitable for suppliers, PSOs with similar needs would benefit from collectively buying the software once and then procuring the services needed to operate and use the solution.

The regional governments have, e.g., for several years developed and maintained a national service platform for hosting, sharing and managing health data. The suppliers have, however, varied over time and been procured, which has forced the market to offer competitive pricing and, by extension, save costs compared to what single-vendor proprietary platform vendors offer.

Studies and quantifications of the economic impact provide an important tool in communicating the value and impact of OSS. There is currently a tool under development at OS2 aimed at quantifying the economic value of OSS software using a widely established effort estimation model for software development. Interviewees

provided examples demonstrating the potential for positive economic upside. One example is the City of Aarhus's migration, where 60 systems were recently moved to a German cloud provider, leading to reduced operational costs from about DKK 800,000 per year to around DKK 225,000 (Kummer, 2025). A planned migration towards OSS office productivity suites is further expected to generate cost savings of up to 7 MDKK by 2029 (Laursen, 2025). Another example, including the proposed school platform OS2skole, estimated to require 26 MDKK for development and 21 MDKK for operations, would break even and create significant cost savings after one year post-deployment, compared to extant licensing fees to incumbent vendors (OS2, 2025).

A further, aligned argument iterated amongst interviewees is that by promoting and acquiring solutions from domestic and European service suppliers, investments are made in growing capabilities, which, over time, will further strengthen strategic autonomy. One study (Asterès, 2025) reports how "*80% of total spending on cloud software and services for business use in Europe went to US companies, representing a volume of €265 billion.*" The study further argues that the spending "*relating exclusively to cloud software and services for business use, represents approximately 2 million direct, indirect, and induced jobs in the US.*" Moreover, "*if 15% of this spending were retained within the European economy by 2035, around 500,000 direct, indirect, and induced jobs would be created, benefiting the European economy*".

5 Barriers and challenges (RQ2)

Summary

Our study highlights structural, organisational, and market factors as the main barriers and challenges currently limiting systematic use and reuse of OSS in Danish public administration. Specifically, these include:

- Strategic misalignment within and between government levels. Initiatives run in parallel without shared foundations, leadership support is inconsistent, and defaulting to familiar incumbents weakens momentum.
- Market power and procurement culture reinforce lock-in. Incumbent influence shapes choices, while seed funding for OSS alternatives is hard to mobilise at the scale required.
- Limited organisational and technical capacity after years of outsourcing. Many PSOs lack the skills and routines to adopt, maintain, or contribute upstream in a sustained way.
- Usability, security, and operational risk perceptions persist, and short-term productivity concerns often outweigh longer-term benefits in sovereignty and flexibility.

Below we elaborate these barriers and how they manifest across strategy, procurement, capability, and day-to-day operations.

5.1 Strategic and leadership misalignment

A recurring challenge concerns a mismatch between ambition, prioritisation, and leadership commitment. This includes a stringent need for coordination among different initiatives and plans to migrate public digital infrastructure to OSS. Different routes emerge from the interviews and should be aligned at both the municipal and national levels. This becomes evident in the parallel yet disconnected sovereign desktop solutions, which miss out on both innovation and opportunities. While there may be room for several options, all stakeholders should collaborate on the foundations, which can later be customised to each specific need.

At the same time, management support is often reported as fluid or missing. Many describe resistance to strategic input from technical experts, combined with general risk aversion and limited understanding of digital infrastructures. Without consistent support, strategies and policy documents fail to create the organisational or cultural momentum required. Even when support exists, it may be withdrawn after leadership changes, as in one case where a long-running LibreOffice deployment was reversed by a new IT manager and replaced with an incumbent solution.

Compounding this is a widely internalised view of Denmark as a “Microsoft-land,” where PSOs default to what is familiar and trusted. Combined with a narrative of

wanting to use “what everyone else uses,” this creates a perception that deviating from traditional incumbent service suppliers is abnormal, risky, or inconvenient.

5.2 Market power, procurement culture, and structural lock-In

Many interviewees point to the strong lobbying efforts of incumbent vendors who see OSS as a threat to their business models. Their influence, spanning financial, relational, and political domains, reinforces a conservative procurement culture in which PSOs remain locked into legacy ecosystems.

Funding structures further deepen this lock-in. Seed funding is often needed for key OSS projects, particularly when too few PSOs are willing to commit upfront due to risk aversion or uncertainty. The OS2skole case illustrates this well: even when long-term savings and independence are clear, the short-term funding required to initiate development is still unattainable. Municipal pooling can only cover initial analyses; large-scale development remains out of reach without broader commitment. The same applies to the Agency for Governmental IT Services, which can only justify OSS investments if enough pilot customers are willing to co-sponsor early development.

There are also concerns about vendors appropriating publicly funded OSS code and integrating it into commercial offerings without contributing back. While licensing strategies and community-building can mitigate this, interviewees nonetheless see it as a risk that needs deliberate management.

5.3 Organisational and technical capabilities

PSOs often lack the internal technical capacity required to adopt, maintain, or meaningfully contribute to OSS solutions. This is partly the result of decades of outsourcing and reliance on consultants, particularly in local governments with limited resources and a narrow operational scope. Existing IT departments are frequently described as competent but overstretched, focused on compliance efforts such as NIS2 and daily operations rather than innovation.

Moreover, effective OSS adoption requires investment in governance, maintenance, and collaborative development. These activities extend far beyond simply “installing software.” They require institutional commitment, sustained engagement, and the ability to contribute back upstream, capabilities that many PSOs do not yet have. Questions also arise around when software is mature and secure enough to release, given concerns about leaks, quality assurance, and reputational risk.

Here, service suppliers still (and will continue to) fill an important void and role for operations, support, and risk mitigation. However, OSS-capable suppliers are still too few to meet the sector’s demands, according to the interviewees. For some PSOs, OSS is still perceived as “community-driven only,” effectively disqualifying it during procurement even when professional support is available. Interviewees describe this as a chicken-and-egg problem: PSOs claim there are no viable suppliers, while suppliers

argue that demand has never been sufficient to justify scaling. Without increased public-sector uptake, supplier capacity will remain limited, and vice versa.

5.4 User experience, productivity, and perceived operational risk

Usability and integration remain practical concerns for many potential adopters. Interviewees note that even minor decreases in ease of use or interoperability can translate into measurable productivity losses when scaled across thousands of employees. These perceived costs are difficult to justify within existing budget frameworks, especially when short-term efficiency takes precedence over long-term sovereignty or flexibility.

Security, sustainability, and maintenance concerns add complexity to these perceptions. OSS is variously seen as both more secure and less secure than proprietary software, depending on the respondent. What emerges is less a question of intrinsic quality and more one of governance: security and sustainability depend on who maintains the code, how actively the community contributes, and whether reliable support arrangements are in place. For professional support and risk mitigation, adopters should consider contracting service suppliers or maintainers of the individual projects.

6 Capabilities required (RQ3)

Public-sector OSPOs essentially constitute a source of expertise and cultural change, and help grow the capabilities needed for their overarching organisations to leverage OSS as a tool for achieving their goals and vision. Specifically, we identify ten specific capabilities needed, and that should be considered and evolved through a national support structure:

Policy translation and strategic advice – Interpreting EU legislation and national priorities, and helping develop OSS strategies and governance models, while aligning cross-government policies on OSS and related areas and topics, including cloud, AI, data governance and security.

Design and operationalisation of policy instruments – Guiding when source code ownership is needed, and how necessary control mechanisms can be created including and beyond OSS; providing procurement guidance and hands-on support, while maintaining essential templates and resources; enabling decision-making for OSS release; supporting project initiation and community development; strengthening sustainability and supply-chain risk management; and preparing organisations for emerging areas such as open source AI, and use of Agentic AI-support in software development.

Investment, prioritisation and scaling - Facilitating and promoting strategic seed funding and impact demonstration, as well as maintenance funding for critical digital infrastructure; developing prioritisation frameworks and migration pathways, and enabling joint agreements and coordinated rollouts.

Shared digital collaboration infrastructure – Establishing, growing, and governing a national government social code collaboration platform and OSS solution catalogue with related communities, templates, resources, on-ramps and taxonomies.

Licence compliance management - Providing routines, tools and guidance to ensure compliant OSS intake, SBOM-based monitoring, pre-release checks and ongoing auditability.

Stewardship of public-sector OSS projects - Ensuring long-term sustainability and shared governance through association-based, supplier-based, internal, or state-owned stewardship models.

Measurement and follow-up - Tracking adoption, reuse, project health, and compliance to guide risk management, improve infrastructures, and inform iterative policy refinement.

Inner Source enablement - Supporting internal and cross-government code sharing and collaboration to build open-working habits before full external release is feasible; enabling government-internal sharing of assets deemed unfit for open dissemination and reuse.

Advocacy and community building - Driving cultural change, building trust, and convening communities of practice across PSOs, suppliers, and civil society to normalise OSS collaboration.

Training and competence development - Providing role-specific capability building and training for policymakers, procurement officers, developers, legal teams, security specialists and end-users.

Below, we further detail how these capabilities might look and how public-sector OSPOs serve as a focal point for their development and provisioning. For each capability, we detail several elements based on interviews and our previous work on public-sector OSPOs (Linåker & Nummelin Carlberg, 2024; Linåker & Muto, 2024).

6.1 Capability to translate and shape open source policy and strategy

Summary

The OSS policy and strategy for an organisation are typically owned and decided upon by policymakers and executives. These, however, seldom have expertise on the topic, which is why public-sector OSPOs serve as an important source of input, often for the design of policies and strategies. The OSPOs are typically also those responsible for the execution and follow-up of the plans laid out.

Specifically, we find in the context of translating and shaping OSS policy and strategy that public-sector OSPOs should consider:

- acting as the bridge between policy and practice, translating EU rules and initiatives into national, regional and local context, participating in consultations, and engaging in European collaborations such as EDIC-DC and the European Commission's OSPO network to align shared assets like the EU OSS catalogue.
- engaging in European standardisation and related community efforts, monitoring and contributing to the development of harmonised standards led by the ESOs to ensure that emerging technical specifications reflect OSS development practices and public-sector needs.
- providing strategic advice to policymakers and leadership, turning technical concerns into policy-ready narratives on sovereignty, interoperability and economic impact, and proposing instruments that can gain traction in risk-averse environments.
- supporting institutions in developing OSS strategies, objectives, governance models and follow-up, and helping prioritise investments by assessing expected benefits, risks and costs.
- coordinating across government and adjacent policy domains, ensuring that OSS-related efforts reinforce wider national goals on cloud, AI, data governance and security rather than evolving into parallel or conflicting initiatives.

Below, we detail the responsibilities public-sector OSPOs need to take on, and the forms of support required.

6.1.1 EU regulatory implementation and EU-level engagement

EU legislation and standardisation are increasingly impacting how digital infrastructure and services are developed and provided. Public-sector OSPOs should coordinate, act as an interface, and help translate such policies and guidelines into national, regional, and local government contexts. The Cyber Resilience Act (CRA) is a clear example of legislation currently undergoing implementation and standardisation efforts, placing new responsibilities on both manufacturers and stewards of OSS software. Upcoming legislations, such as the Cloud and AI Development Act and the European Commission's OSS strategy (also referred to as the European Open Digital Ecosystem Strategy[1]) are other initiatives that come with additional requirements and recommendations that will need support to be implemented and adopted by concerned actors, both on the buyer and supplier side. Public-sector OSPOs interviewed describe how they both actively participate in consultations, and act as a bridge in the translations between EU policy and national implementation. They further emphasise the need for increased collaboration with community actors, such as national business alliances in helping with the translation and implementation of EU acts, such as the CRA.

Public-sector OSPOs also need to monitor and engage with various European initiatives that support the use of OSS in line with their countries' strategic goals and vision, e.g., those related to digital sovereignty. The European Digital Infrastructure Consortium for Digital Commons (EDIC-DC)[2] exemplifies this, inviting national governments to collaborate on the governance and development of digital commons. The EDIC-DC is described by public-sector OSPO interviewees as a strategic hub for cross-government collaboration and as key to Europe's digital sovereignty. The flagship project currently centres on the development of office productivity suites, including overlapping solutions from France (La Suite Numerique[3]), Germany (OpenDesk[4]) and the Netherlands (MijnBureau[5]). Engaging either as a participatory or observing member would be beneficial for Denmark considering ongoing work with sovereign desktop solutions through the Agency for Governmental IT Services (Statens IT) and OS2.

Another important community is the European Commission's OSPO network[6], which brings together many of Europe's public-sector OSPOs to collaborate on developing joint best practices. All public-sector OSPO interviewees are actively engaged in the network and praise its importance for sharing knowledge and initiating joint projects. Overlapping projects include the EC's OSS solutions catalogue[7], and public-code.yml[8], a

[1] https://digital-strategy.ec.europa.eu/en/news/commission-opens-call-evidence-open-source-digital-ecosystems
[2] https://digital-strategy.ec.europa.eu/en/news/commission-launch-digital-commons-edic-support-sovereign-european-digital-infrastructure-and
[3] https://lasuite.numerique.gouv.fr/
[4] https://www.opendesk.eu/en
[5] https://minbzk.github.io/mijn-bureau-infra/
[6] https://interoperable-europe.ec.europa.eu/collection/eu-ospo-network
[7] https://interoperable-europe.ec.europa.eu/eu-oss-catalogue
[8] https://github.com/publiccodeyml/publiccode.yml

meta-data standard for public-sector OSS. Both projects are important for promoting findability and enabling cross-border reuse as motivated by the Interoperable Europe Act.

6.1.2 Engaging in European standardisation efforts

Standardisation is a commonly used means of implementing EU digital regulation by translating high-level legal obligations into concrete, testable, and interoperable requirements. This translation helps create a shared technical reference that ensures predictable compliance pathways and alignment across borders and stakeholders. Three European Standardisation Organisations (ESOs) are typically used as vehicles for the standardisation efforts: CEN (the European Committee for Standardisation), CENELEC (the European Committee for Electrotechnical Standardisation), and ETSI (the European Telecommunications Standards Institute). These are formally mandated to develop harmonised standards and related specifications, ensuring that legislative objectives are operationalised consistently and in a technology-neutral manner across the EU.

As digital legislation is increasing, public-sector OSPOs need to actively monitor the European standardisation processes and engage accordingly to ensure that emerging standards reflect OSS development practices, licensing models, and governance realities. Engagement enables OSPOs to anticipate regulatory requirements, contribute to shaping interoperable and open technical ecosystems, and protect the sustainability of OSS collaboration by ensuring standards do not inadvertently privilege proprietary development models or impose disproportionate compliance burdens.

For the CRA, as an example, standardisation plays a central role in translating the Act's lifecycle-oriented cybersecurity requirements into implementable technical expectations. This includes developing horizontal standards for general cybersecurity principles and vulnerability management, as well as vertical standards tailored to specific categories of digital products. These standards support manufacturers and OSS stewards in understanding how to demonstrate compliance and in navigating regulatory concepts that would otherwise remain high-level and abstract. The engagement from groups such as the Open Regulatory Compliance Working Group[9] (ORC WG) and the recent addition of representation from OSS communities to the ESOs is playing a pivotal role in shaping the standards, although the process is still reported as sensitive. As a first action, public-sector OSPOs should engage with organisations such as the ORC WG and the EU OSPO network to monitor and identify suitable engagement approaches.

For specific OSPOs, it may also be important to consider other standardisation processes not specifically related to OSS, but to data sharing and broader forms of interoperability. One interviewee highlights the health care domain and challenges with standards designed without insight or influence from the perspective of Danish PSOs.

[9] https://orcwg.org/

6.1.3 Strategic input and advisory support to policymakers

There is a general feeling that political guidance and policy are required for substantial change to happen, related to enabling the use of OSS as a means towards goals such as increased digital sovereignty, interoperability, and economic impact. For such policies to happen, policymakers require input of relevant data, motivations and examples. Any input must also manage an atmosphere described as risk-averse and, at times, resistant to strategic advice.

Public-sector OSPOs provide a suitable source and facilitator of such advice, and can support drafting and shaping of strategic frameworks and policies on the use of OSS in alignment with policy goals. One public-sector OSPO interviewee describes their role as a storytelling and sense-making unit for policymakers, translating technical topics into political narratives and supplying input on sovereignty. Several public-sector OSPO interviewees exemplify how they actively provide input to policies such as the national digitalisation strategy, cloud strategy, and digital autonomy. OSS is consistently promoted for inclusion as a tool and output where appropriate, though never as a topic or goal in itself. Formal connections to national, regional, and local parliaments are, hence, important for tackling the challenges highlighted.

Support and input are also needed on the local and regional levels of government, where national or regional OSPOs could play an important role. OS2, as an Association-based OSPO, already provides a close proxy, as they organise most municipalities for OSS collaborations. With extended resources and mandate, they could potentially take on a wider role going beyond their current stewardship focus as part of any national or regional OSPO structure.

Resourceful entities, such as the City of Aarhus, may be able to set up their own support structures. The city at hand has been a clear and strong presence of internal capabilities and know-how, which has supported and been reflected in policy since the City's first OSS strategy (Aarhus commune, 2014). A recent policy pushes the City to gradually migrate away from proprietary desktop suites toward OSS alternatives, driven by digital sovereignty and rising licensing costs from current vendors. Municipalities and PSOs, which are less resourceful, will require support.

Regardless of the level of government, strategic investment decisions for new and existing OSS projects will require in-depth knowledge of valuing expected benefits against potential risks and costs, and of prioritising and implementing funding decisions accordingly. Here, public-sector OSPOs should provide such support, help decision-makers prioritise where investments go based on national strategies and policies, and support follow-up on impact and continued execution.

6.1.4 Institutional open source strategy development

While policymakers at various levels of government can provide overarching direction and policy, strategic intent and leadership are still needed at the organisational level. Executive support and sponsorship by, e.g., CIOs, and the detailing of how OSS can and should be used in line with the organisation's business strategies are critical. At the policy level, such leadership or strategies are generally lacking, according to the interviewees. The Dutch national government OSPO describes a setup in which a cross-

governmental CIO office coordinates CIOs across the various national ministries, acting as a funnel to develop and align OSS policy at the national level of government.

Public-sector OSPOs, in this regard, act as intermediaries that convert broad political commitments and legal requirements related to OSS into concrete, actionable yet general practices and guidelines for PSOs. In parallel, public-sector OSPOs may also support PSOs independently in developing their own OSS strategies that align with national goals while reflecting local needs and capacities. This may involve co-defining objectives, governance models, and follow-up mechanisms, or embedding OSS considerations within broader digital transformation agendas when formal strategies are absent. As earlier reports show, this can quickly become a scaling issue if the task is tied to one single OSPO (Linåker et al., 2024).

Public-sector OSPO interviewees generally describe different forms of advice and consultancy work to support the drafting of OSS strategies or the inclusion of OSS across relevant policies. One public-sector OSPO describes how it translates the annually revised OSS strategy into operational goals for the concerned PSOs and municipalities within its jurisdiction.

6.1.5 Cross-government coordination and alignment with broader policy goals

Effective support for OSS adoption in the public sector requires coordinated efforts across all levels of government. As capabilities mature, support structures must be synchronised to ensure they remain complementary rather than fragmented, enabling PSOs to access coherent guidance, shared resources, and aligned processes. OSPOs across PSOs and levels of government need synchronisation and coordination mechanisms to ensure strategy alignment and synergies between efforts so that their work collectively contributes to overarching goals and visions related to, e.g., digital sovereignty.

Sweden and the Netherlands exemplify how national OSPO networks have emerged, encompassing both public and private organisations. These help disseminate knowledge and develop shared practice, while also growing communities of coordination and the exploitation of joint projects at the national level. The Dutch OSPO structure, set up through their national ministerial CIO office, also provides a means to coordinate support and policy at the national level. Schleswig-Holstein exemplifies a dual OSPO structure: a formal, central entity that supports and coordinates state-level efforts, whilst a virtual OSPO, comprising different subject matter experts, supports PSOs across the state at a wider, especially municipal, level. Together, the two OSPOs maintain a task force, which also includes other key stakeholders, such as their public service provider and development teams.

This coordination needs to extend beyond the immediate remit of OSS, with OSPOs actively linking their work to broader national objectives, such as digital sovereignty. This includes the wider technological ecosystem, encompassing the development and procurement of AI models and cloud services, hardware design and manufacturing, and control over critical communication infrastructure. Several public-sector OSPO interviewees confirm their involvement across different types of policies and thereby

engage with other government functions. For this reason, OSPOs must operate with a clear mandate to collaborate with adjacent initiatives and policy functions, ensuring that OSS efforts are integrated into, rather than isolated from, the wider strategic landscape.

6.2 Capability to design and operationalise policy instruments

Summary

Public-sector ambitions for OSS depend on policy instruments that are clear, actionable and consistently applied. The investigation shows that current instruments are fragmented, advisory in nature, and difficult for PSOs to operationalise without additional support.

Specifically, we find in the context of designing and operationalising policy instruments that public-sector OSPOs should consider:

- helping PSOs navigate prescriptive and advisory models, clarifying when OSS should be considered first, how open-unless principles apply and how ownership, release decisions and open standards obligations are interpreted in practice.
- advising on ownership and control mechanisms, guiding when source code ownership is needed to enable sharing and reuse, and when interoperability, open standards, and exit and preparedness strategies provide sufficient control without ownership.
- supporting the creation and maintenance of standardised procurement requirements and contract templates, shaping procurement language, scoring models and qualification criteria, and contributing to shared repositories of examples.
- providing procurement guidance and hands-on support, assisting procurement officers in evaluating OSS options, selecting licences, designing requirements and understanding safe release or acquisition pathways.
- enabling decision-making for OSS release through structured processes that address maturity, security, sensitivity and business value.
- supporting project initiation and community development, with guidance, training, governance templates and community-building practices.
- strengthening sustainability and supply-chain risk management by promoting methods for evaluating project health, maintainability and dependency risks, including SBOM-based approaches.
- preparing organisations for emerging areas such as open source AI, helping interpret transparency, data provenance and reproducibility requirements while avoiding new forms of dependency.

Below, we expand on the instruments, processes and support mechanisms needed to enable consistent policy implementation across government.

6.2.1 Policy approaches: prescriptive and advisory models

Prescriptive OSS policies require that OSS be considered first-hand in the acquisition process or used as a release mechanism for any software developed with public funding (Linåker & Muto, 2024). Advisory policies recommend but do not require such actions. Both approaches come with pros and cons.

Some interviewees promote prescriptive policies as the only way to create change. PROSA[10], e.g., advocates for introducing requirements in procurement templates that, whenever PSO procures software development, it should be considered for release as OSS by default. Exceptions should still be possible when explanations can be provided. Failure to comply should be met with some form of consequence. When reviewing contracts, PSOs need to review the original rationale for why software is not released as OSS and assess whether and why it is still valid. When buying custom off-the-shelf software, requirements should be more relaxed, although OSS alternatives should be actively investigated.

In the Netherlands (similar to, e.g., Kenya and France), an open-unless policy is in place, but its adoption has been limited due to a broad interpretation of its requirements (Wet open overheid, 2023). A similar critique was raised by one interviewee, stating that prescriptive policies will only generate various excuses and standardised means of avoiding compliance. The same interviewee, as well as others, promotes a more pragmatic approach in line with advisory policies, where there should be a business case for the decision at hand, i.e., the expected value outweighs potential costs and risks. There is also a need to recognise that an end goal can be achieved through several means, and that OSS is only one of them. Achieving necessary control and interoperability may, e.g., be done by requiring the use of open standards for data formats and system interfaces, and by securing unrestricted access to and ownership of the concerned data.

Extant policies in Denmark, both for inbound and outbound cases, are generally advisory. The guidelines authored by the Agency for Digital Government encourage and support the adoption and release of OSS for state-level PSOs (Digitaliseringsstyrelsen, 2022a), echoing findings and proposals from the software strategy authored by the National Technology Council in 2002 (Teknologirådet, 2002).

The national IT project guidelines also emphasise, in their principles, that procured or developed software should be based on the reuse of existing solutions to the greatest possible extent (Digitaliseringsstyrelsen, 2022b). If there are no existing solutions that can be used as is, customising existing solutions should be preferred before developing a solution from scratch. Similar encouragement is provided by the national principles from 2014, which highlight that public-sector software should be released as OSS to enable reuse as far as possible (Digitaliseringsstyrelsen, 2014).

[10] https://www.prosa.dk/english

6.2.2 Ownership models to enable sharing and reuse

The outbound case of developing new software through internal or external resources is highlighted by several as a key concern, with current policies considered lacking. The latter should be contrasted with national architectural principles, which essentially promote sharing and reuse, although on an advisory, rather than prescriptive level (Digitaliseringsstyrelsen, 2022a,b).

Several interviewees favour a more articulated stance and recommendation on the ownership of the source code as an enabler for sharing and reuse of software across PSOs. The decision on whether to OSS can accordingly be made on a case-by-case basis, considering specific concerns and conditions. Ownership is argued to enable PSOs to take control of both the software and the processes for its development and maintenance, while suppliers can still be a key source of the technical capabilities needed.

The Irish government outlines in its key IT Service Provider contracts that ownership of any IP belongs to the Government as customer and Service Providers are expected to open source key codebases as contributions to open digital commons. Ownership is considered a key enabler of ensuring the openness, and flexibility in switching between vendors and in avoiding the risk of lock-in. Similar recommendations can be found in countries such as New Zealand, which recommends IP ownership unless special conditions apply (Linåker & Muto, 2024).

One interviewee proposes a middle-ground approach: prescribing a certain percentage of new software developed for release as OSS. The City of Aarhus provides an example with its recent announcement and intent of migrating 25% of its users to OSS office productivity suites by 2030 (Laursen, 2025). Another proposal includes requiring all projects with budgets over 50 MDKK to be publicly archived and shared. Projects beyond that limit today need to bypass the Danish central government's IT Council (Statens IT-råd[11]), which advises ministries on major IT projects and provides professional risk assessments and reviews of large state IT projects and agencies' IT system portfolios.

6.2.3 Control mechanisms without ownership

Other interviewees point to the need of ensuring and enforcing control, which does not necessarily have PSOs' ownership of the software as a pre-requisite. Control can instead be enforced by promoting interoperability and ease of replacement, and putting in requirements on, e.g., the use of open standards, provisioning of free and unrestricted access to data, and/or release of source code as OSS – methods also prescribed by extant research (Lundell et al, 2021a).

Several interviewees also raised the need to define exit strategies up front, which constitute a plan for switching out a system, detailing risks and costs. Such plans, also referred to as exit strategies (Lundell et al., 2021b), need to be factored into the overall procurement and acquisition process and evaluation. Interviewees also highlight the

[11] https://oes.dk/it-og-oekonomistyring/statens-it-raad/

need for preparedness strategies that align with exit strategies in purpose but focus specifically on cases where a PSO will need to switch to an alternative solution, e.g., in a crisis when response time is short, and the need for action is urgent. Both types of strategies should be defined by the procuring PSO(s) or be required of the service supplier.

Open standards are also highlighted by several as another tool to be considered alongside OSS for enabling open and interoperable solutions. According to some interviewees, open standards are not considered as controversial or technical as OSS, and easier to grasp and adopt in practice, e.g., in the context of an acquisition and procurement process. Some interviewees praise previous Standardisation Office within the Danish Agency of Digital Government (Digitaliseringsstyrelsen) for attempts in standardising file formats in the public sector, including Open Document Format[12] used by LibreOffice[13], an OSS office productivity suite.

Introduction and enforcement of corresponding or aligning requirements in general frameworks such as the "Fællesoffentlige digitale arkitektur (FDA)" as a minimum level is proposed by some interviewees, implying that the bar should be raised in terms of making some principles prescriptive and some advisory compared to the current case which is generally on an advisory level (Digitaliseringsstyrelsen, 2022a,b). One interviewee states a goal of 5-15 years all systems should be deemed as interoperable, and exchangeable, again highlighting quotas as a means to progress.

On a European level, frameworks such as the Cloud Sovereignty Framework (European Commission, 2025) from the EU is emerging and growing in adoption[14], providing a standard means for how tenders and suppliers can be evaluated in terms of different sovereignty dimensions and levels. Legal accountability (e.g., ownership structure and location of head office), data sovereignty (e.g., where and how data is stored, managed and potentially encrypted), and technical portability (e.g., use of OSS and open standards) are some of the aspects considered. Public-sector OSPOs should continuously monitor the European developments, and consider how such frameworks and practice can be applied in the Danish context.

6.2.4 Standardised requirements and contract templates

The introduction of examples or optional requirements into procurement templates and frameworks used by PSOs is viewed by interviewees as a means to significantly lower the barrier to considering OSS as a sharing and reuse mechanism.

As mentioned earlier, the introduction of standardised requirements around support for OSS Building Blocks as Digital Public Infrastructure is having a transformative impact on the Irish government's IT infrastructure. The German Centre for Digital Sovereignty (ZenDIS) is currently in a process of collecting example tender documents and is pushing for the creation of new or updated standard procurement contracts that consider OSS specifically.

[12] https://blog.documentfoundation.org/blog/2025/05/16/what-is-odf/
[13] https://www.libreoffice.org/
[14] https://www.techzine.nl/nieuws/infrastructure/576017/dienst-ict-uitvoering-lanceert-toetsingsinstrument-voor-soevereine-cloud/

In Denmark, the standard contracts for IT project procurement, K1-K4[15], supplied by the Danish Agency of Digital Government (Digitaliseringsstyrelsen), are pointed out as an important target for such requirements. These contracts are, however, no longer maintained and may need considerable revision to remain applicable. Yet, they symbolise a source of knowledge and trust that PSOs request and need when entering a procurement process.

An alternative solution is presented by the "Standard and methods for requirements and acquisition project", which proposes a platform with related governance for stewarding and collecting example requirements, procurement templates, and general knowledge sharing for public procurement of IT projects (Digitaliseringsstyrelsen, 2024). Such a platform, preferably maintained by a neutral and long-term host with the interests of all levels of government in mind, would provide a valuable source of support for both the adoption and release of OSS.

Central procurement bodies, such as SKI (Staten og Kommunernes Indkøbsservice A/S) and the Advisory Unit for Procurement Program under the Agency for Public Finance and Management (Rådgivningsenheden Statens Indkøb[16] - Økonomistyrelsen) that hold standardised framework agreements, e.g., including standard software, as well as support and hosting services, are also well placed as key implementors of optional share and reuse requirements. In the case of SKI (n.d.), a target for such optional requirements could be "Standard Appendices for Usage Requirements", which already contains requirements permitting certain reuse, while limited to inter-organisational sharing across PSOs (c.f. SKI, n.d.).

Equally important is to consider the scoring systems of tenders and qualification requirements of suppliers, which must also be revised to consider the context of OSS specifically. The German Open Source Business Alliance (2025) has proposed four such criteria, focusing on evaluating a supplier's experience and track record of contributing to and engaging with relevant OSS projects and their dependencies.

From a supplier perspective, while some may express reluctance, most interviewees agree that service suppliers will become accustomed to what to expect in tenders and how to customise their offerings and responses accordingly. With time, this will further increase bid quality and competitiveness. The Irish experience from procuring services of three different vendors has shown a positive sign in how quickly they adapted to the new conditions.

6.2.5 Procurement support and practitioner guidance

Standardised requirements and contract templates are one thing, but knowing when and how to use them is another. Support and guidance in the procurement process are central to enabling OSS adoption and release, as exemplified by Italy (Linåker et al., 2024). While having an open-by-default prescriptive OSS policy since 2012, it did not have any significant impact or conformance until its procurement guidelines were released in 2019. Such guidelines cover aspects such as ownership of intellectual

[15] https://digst.dk/it-loesninger/standardkontrakter/
[16] https://oes.dk/indkoeb/gaeldende-aftaler-i-statens-indkoebsprogram/

property (e.g., source code), license selection, and where and how software is to be developed and released.

Hands-on support and consultancy are highlighted as practices across National Government OSPOs in France and Germany (Linåker et al., 2024), and are reiterated in the public-sector OSPO interviews. Questions are typically general but difficult for single procurement officers without the necessary training to answer. Advisory and consultancy are complemented by dedicated training and knowledge-sharing events, e.g., with national OSPO networks.

Providing hands-on support is generally feasible but can become problematic as requests increase, which is why scalable approaches, such as training and guidelines, are recommended. Beyond any formal OSPO in Denmark, SKI and the Advisory Unit for Public Procurement (Rådgivningsenheden Statens Indkøb) provide two potential proxies for such support and advice.

Suppliers and consultancies are also highlighted as sources of support for the procurement process, both hands-on and through training and education for IT managers and procurement officers. These can be sourced as experts in the requirements engineering and specification process, to support tender evaluation, and to test and verify requirements in the solutions procured. OS2 commonly uses a second supplier to verify the quality of a release from a primary supplier and to confirm that all artefacts required for the solution to be "open source" in the sense that it can be transferred to another vendor are present.

Capabilities among IT departments in PSOs in adopting and operating infrastructure tools and services, typically through suppliers, are also highlighted by several interviewees as a critical source of subject matter expertise. By leveraging these as experts in procurement processes, procurement officers can gain valuable technical input and local contextual knowledge of IT operations.

IT departments, especially on the local government level, are, however, also recognised as limited in capacity. Pooling and sharing technical expertise can, hence, also be an option, e.g., through OS2 or shared supplier contracts.

6.2.6 Decision support for open source release

The question of whether software should be released as OSS in the industry is a decision that considers business value against potential costs and risks (Linåker & Regnell, 2020). Expected benefits do not come automatically and can be easily erased and outweighed by a negative backdrop. This also holds true for the public sector, where the decision to open source is typically guided by policy, which is either prescriptive, advisory, or more akin to high-level endorsements (Linåker & Muto, 2024).

For prescriptive open-by-default policies, (national) security, integrity and privacy are common conditions warranting negative decisions, while the business case at hand is more commonly a driver under more permissive and advisory policies. Regardless of the type of policy, interviewees raise concerns about knowing when to release as OSS.

The concerns are typically expressed from a security standpoint, e.g., when the software is considered too sensitive or critical to open up due to the risk of exploitation, and how and to what extent it should be tested and quality assured. Explicit guidelines, processes, and hands-on support are required on a case-by-case basis, as several interviewees noted.

Looking across Europe, several examples can be found (Linåker & Muto, 2024). In the Netherlands, for example, the Ministry of the Interior and Kingdom Relations has developed process charts and detailed guidance to support its "Open, unless" policy (Procee et al., 2022). In France, the Free Software Unit provides three criteria related to the software's usability for other OSS projects, the general need for it, and the technical profile of end-users (Direction Interministérielle du Numérique, 2023). Based on the criteria, they propose four levels of openness for how the software may or should be shared.

In the UK, the Government Digital Service maintains a Service Standard that specifies the requirement for public authorities to "[m]ake new source code open" in order for people to reuse and build on" the code, notably by publishing the code in an open repository and retaining ownership of the associated intellectual property rights, making it available for re-use under an open license (Government Digital Service, 2022). It provides more detailed guidance on implementing this requirement in the Service Manual (Government Digital Service, 2017).

In Denmark specifically, there is currently no law or general policy prescribing whether publicly funded software should be released as OSS. There are, however, guidelines authored by the Agency for Digital Government that encourage and support the release of OSS for state-level PSOs (Digitaliseringsstyrelsen, 2022a), echoing findings and proposals from the software strategy authored by the National Technology Council in 2002 (Teknologirådet, 2002). While recognised by interviewees, current guidelines still lack clarity compared to those of other countries regarding what is necessary to guide PSOs in deciding whether to release software as OSS.

6.2.7 Guidance for project initiation and community development

Interconnecting and following the decision to OSS a solution, whether for an existing project or a new one, there is a need for support and guidance, as it can be a complex journey. While capabilities and know-how can be procured as suggested by some interviewees, it is also important to have internal capabilities to manage OSS projects and their communities. Here, the public-sector OSPOs fill an important void with support that needs to scale, just as in procurement, through both hands-on consultancy and more general resources, such as training programs and guidelines.

Looking internationally (Linåker & Muto, 2024), many guidelines offer rich guidance, such as those in New Zealand (New Zealand Government, 2016) and France (Direction Interministérielle du Numérique, 2023). In Denmark specifically, there are some guidelines present that can support PSOs in the release process. Guidelines from the Agency for Digital Government (2022a) discuss licensing options and how to develop, collaborate, and establish a sustainable community. Further and complementary

guidelines are also provided in earlier publications (Digitaliseringsstyrelsen, 2014; Teknologirådet, 2002). OS2 further provides standardised processes for the collaborative development and maintenance of OSS projects among its members (Frey, 2023) and supports the implementation of municipal-level architectural principles (Kommunernes Landsforening, n.d.).

6.2.8 Sustainability and supply-chain Risk management

PSOs must learn to understand the dynamics of the development and long-term maintenance of OSS, the risks that arise when adopting it, and how to systematically analyse and address those risks. Such considerations are necessary both when selecting individual OSS components for everyday development work and when evaluating larger systems during acquisition and procurement processes. Importantly, the need for continuous assessment does not end after adoption; OSS projects evolve quickly, and their health, activity, governance, and risk profile can change over time.

An OSS project's "health" is multifaceted and cannot be reduced to a single metric; it encompasses its long-term viability, maintenance capacity, community productivity, robust governance, and openness to contributions (Linåker et al., 2024). Assessing these characteristics requires treating health checks like diagnostic procedures, in which the adopter must identify symptoms, ask structured questions, analyse root causes, and determine whether action is required (Germonprez & Linåker, 2024). Tools and frameworks can support this process by providing checklists and structured metrics, but they must be paired with contextual, manual analysis by individuals who understand how different OSS communities, governance structures, and development contexts vary. The Italian procurement guidelines, e.g., integrates a part on how health can be assessed, and equally compared and contrasted across OSS alternatives. Health assessments are also important when comparing against proprietary options, and considering what type of support may be needed and should be acquired accordingly.

The German Centre for Digital Sovereignty (ZenDIS) considers supply-chain security a top concern and addresses the topic through its national social code-collaboration platform, OpenCode, where all public-sector OSS projects are collected. The platform provides automated compliance and security scanning tools, which support decisions on whether a codebase is mature enough to open. Software Bills of Material (SBOMs) are generated automatically to provide transparency and health checks into the dependency trees of shared OSS projects.

Still, the adoption of tools and practices is rather limited across Europe, both in the public and private sectors. Here, public-sector OSPOs, exemplified by ZenDIS, need to grow and maintain practices that can scale across PSOs and procurement practices, while promoting collaboration and knowledge sharing. Sharing assessments across PSOs and vendors, and using common frameworks for OSS health evaluation, can strengthen collective risk awareness and improve the resilience and security of public-sector IT infrastructure.

6.2.9 Policy considerations for open source AI

There is an increasing need for PSOs to also consider the use and development of open source AI. This adds further complexity by considering the many artefacts and inputs that go into the creation and maintenance of an open source AI system.

For PSOs aiming to procure a system, requirements need not just to consider the license of the model, but also consider quality, copyright and provenance of data used for training, evaluation and benchmarking, as well as transparency and availability of documentation and infrastructure necessary to reproduce, follow, and assess the quality of the training for any AI model.

These and many more aspects overlap with the capabilities needed for OSS, which is why any support structure should not limit itself to OSS. Still, none of the surveyed public-sector OSPOs considers it a primary focus, though it remains an important source of input. This is exemplified by the German Centre for Digital Sovereignty, which provided input to the German Parliament on the role of open source AI in relation to digital sovereignty (Zentrum für Digitale Souveränität der Öffentlichen Verwaltung, 2024).

In the report, open source AI is seen as a key instrument to avoid reproducing cloud-style dependencies in AI, by enabling sovereign deployment of models on European infrastructure and reducing oligopolistic control by large tech firms. Open source generative AI models like Stable Diffusion are highlighted as concrete examples that can break emerging oligopolies. The transparency of open source AI, including code and data, is described as its biggest societal advantage, because it allows independent scrutiny, mitigates bias and manipulation risks, and supports AI use that aligns with European values and public-sector requirements.

6.3 Capability to invest in, prioritise, and scale strategic open source alternatives

Summary

Strengthening digital sovereignty and reducing reliance on proprietary systems requires deliberate prioritisation and sustained investment in viable OSS alternatives. Individual PSOs seldom have the mandate, scale, or coordination capacity to do this alone. Public-sector OSPOs are therefore needed to guide where to focus, how to initiate and scale efforts, and how to coordinate action across organisational boundaries.

Specifically, we find in the context of investing in and scaling strategic OSS alternatives that public-sector OSPOs should consider:

- facilitating strategic seed funding (e.g., through tripartite co-funding and micro-investments) and impact demonstration by identifying high-value use cases, aligning cross-government investment, and helping PSOs evidence concrete economic and operational benefits.
- promoting maintenance funding for critical digital infrastructure through structured dependency mapping and prioritisation, ensuring long-term security and sustainability of widely reused components.
- developing prioritisation frameworks and migration pathways that plan stepwise transitions, considering both backend replacements and user-facing changes, guided by feasibility and sovereignty considerations.
- enabling joint agreements and coordinated rollouts to secure scale, align with national objectives, and reduce risk through phased adoption and shared supplier capacity.
- by defining common standards and providing reference implementations based on open standards, OSS, and transparency, that guide how public-sector digital infrastructure should be built with digital sovereignty in mind.
- supporting dual-channel adoption strategies that introduce viable OSS options alongside incumbent systems to reduce dependency while building resilience and bargaining power over time.

Below, we expand on the practices and capability requirements associated with these areas.

6.3.1 Strategic seed funding and impact demonstration

When there is no prescriptive policy in place and the decision is left to PSOs on whether to adopt or release software as OSS, interviewees describe a reluctance among decision-makers to make the necessary investments.

While the OS2 collaboration has demonstrated its impact across 25+ products, projects requiring larger investments still prove difficult. The case of OS2skole[17], a complete OSS workspace solution for schools, is cited by several interviewees who highlight that break-even would be achieved one year post-deployment (OS2, 2025). The project signals the difficulties municipalities face at the national level in agreeing on joint funding, even though the need is both common and critical. From a national government perspective, investments into the project are not prioritised as it is considered a municipal responsibility. In the end, the cultural and siloed mindset keeps the project stuck in the status quo between levels of government.

Several interviewees across levels of government, including representatives from public-sector OSPOs (e.g., the Netherlands and Kenya), recognise the general issue and call for dedicated seed funding to help develop and scale projects that address strategic use cases where alternatives are missing. Funding should also prioritise projects that can demonstrate the potential impact and size of economic and other incentives for going open source.

Several examples show promise. One includes the tripartite co-funding by the Danish government, KL and Danske Regioner of large-scale digital projects by establishing shared national agreements, worth in total, 266.7 million DKK spread across three AI large scale projects – "*storskalaprojekter*" (Kommunernes Landsforening, 2025). One of the projects includes OS2ai, which aims to create an LLM-based AI assistant for civil servants. The project has also received additional funding as part of a EU-funded Digital Europe project. Another example of a similar tripartite collaboration regards the funding of 40 different AI projects, or "*Signaturprojekter*" between 2020-2022 worth a total of 187 million DDK (Digitaliseringsstyrelsen, n.d.).

On the municipal level, there is the example of "*Kommunernes skaleringssamarbejde*" – a joint fund for scaling IT solutions beyond one single municipality (Kommunernes Landsforening, 2025b). Then there is also the broader example of OS2 where 25+ solutions are being actively co-funded by various constellations of municipalities. More isolated investments may also be noted, including the cities of Copenhagen and Aarhus (Interoperable Europe, 2025), the Ministry for Digitalisation, and the Danish Road Traffic Authority (Færdselsstyrelsen, 2025). Still, a coherent cross-government strategy and collaboration are missing.

A dedicated annual fund for innovation projects, e.g., based on a tripartite setup as already demonstrated, could be one approach for providing in-kind or full funding when there is a lack of political support as in the case of OS2skole. One interviewee proposes a model similar to scientific research funds with a yearly budget, which could invest in key OSS projects of strategic importance to Denmark. Initiatives such as the

[17] https://www.os2.eu/os2skole

German Prototype Fund[18] provide a potential model where funding is directed towards innovative OSS projects addressing key concerns defined by the German government, including data security and software infrastructure.

In Schleswig-Holstein, the state government runs a yearly funding program. Although the funding available is relatively modest, its purpose is not to fully finance projects but to give organisations the confidence and encouragement to get started. Early funding rounds supported 14 projects totalling €3 million (around €20–30k per project). The intent is to signal that if a municipality or PSO encounters challenges or needs help on specific OSS topics, the programme will support them by providing expertise and the seed funding required. With more than 100 applications, the programme sees strong demand going forward.

On the national level, the German Centre for Digital Sovereignty (ZenDIS) has moved to take on responsibility for developing both an OSS office productivity suite (OpenDesk[19]), while also providing an OSS-based social code collaboration platform (OpenCode[20]). While taking on the initial risk, the Centre is now adopting a subscription-based business model, providing OpenDesk as a service to PSOs across the country.

The Government Digital Services (GDS) of the UK, according to one interviewee, also demonstrates how a national government OSPO-like function can take on larger-scale development, as in the case of the UK government design system (GOV.UK). The system was initiated by a small team tasked with consolidating 2000+ different UK government e-services, and is now standardised across government. GDS has since expanded its development capacity to other parts of the national digital infrastructure and has recently announced intentions of providing technical support to local governments in adopting relevant parts of it.

6.3.2 Maintenance funding of vital infrastructure

While seed funding is required to initiate key projects, several interviewees also see funding for the maintenance of vital infrastructure components as critical. They recognise that the responsibility for maintaining the digital infrastructure is less clear than for the physical infrastructure, and that the government needs to take on a more explicit and broader role. The German government and its Sovereign Tech Agency are repeatedly referenced across interviews, including by public-sector OSPOs, as models to replicate.

The Sovereign Tech Agency is a publicly funded program that identifies and supports critical OSS projects essential to digital public infrastructure. Its mission is to strengthen the long-term security, resilience, and sustainability of these projects by providing targeted maintenance funding and expert guidance. They use public procurement as a lever to hire individuals already engaged in key projects to do work

[18] https://www.prototypefund.de/en
[19] https://www.opendesk.eu/de
[20] https://opencode.de/en

that is not otherwise possible or prioritised. Since its inception, the funding program has invested around € 23.5 million in 60 critical technologies[21].

A similar funding program in Denmark would be complementary, while taking a national strategic perspective on which technologies are considered critical. Structured dependency mappings and risk analysis of key digital infrastructure should guide the process, with support and prioritisation effort from the OSPOs.

6.3.3 Prioritisation frameworks and migration pathways

Sovereignty and other benefits sought cannot be gained overnight. The transition needs to be made stepwise, as it would otherwise become too complex and costly. Three approaches are highlighted from the interviews. They are not necessarily mutually exclusive, but provide input to planning and prioritising investments and collaborative efforts.

6.3.3.1 Dependency mapping and roadmapping

The first approach centres on a rigorous mapping of dependencies across PSOs in terms of digital sovereignty and potential cost savings, as also proposed by earlier work (PA Consulting, 2026). Based on the criteria, the most critical dependencies are prioritised and analysed to determine how these can potentially be replaced by OSS or alternative solutions. A roadmap should then be formed accordingly and implemented with a long-term horizon and strategic funding.

The Kenyan National Government OSPO is currently conducting a baseline study to identify where and how OSS is used, and where there are opportunities for a switch. The baseline study will accordingly help the OSPO and the national government prioritise their investments and roadmapping process going forward.

The Irish government made an early decision to base their roadmap and investment strategy on a subset building blocks from the GovStack - a modular, open, and reusable “digital building blocks” framework that helps governments rapidly design and scale interoperable e-government services without rebuilding core components each time.

6.3.3.2 Back-to-front replacement (server-side first)

The second approach proposes to start the focus with migrating or replacing modules that are easy to switch out, i.e., the low-hanging fruit, which is typically located on the server side of the digital infrastructure, where there are OSS alternatives widely present and supported. The approach is leveraged in both Trinidad and Tobago and Kenya, where pilots are being conducted to transfer back-end infrastructure from proprietary to OSS solutions

The approach is further characterised as having considerable potential for sharing and reuse across PSOs with large IT investments and operations, such as KOMBIT[22], DBC Digital[23], the Agency for Governmental IT Services[24] (Statens IT) and the Danish Court

[21] https://www.sovereign.tech/press/release-sovereign-tech-agency
[22] https://www.kombit.dk
[23] https://www.dbc.dk

Administration[25] (Domstolsstyrelsen). These organisations also have internal developers and technical capabilities, which are highlighted as key success factors, as they can understand the technical underpinnings of the OSS and integrate accordingly. IT departments in less resourceful PSOs are also described as knowledgeable, though in some cases, additional education and training may be needed.

Remaining dependencies should be mapped out, highlighting what parts are difficult to transition or migrate to OSS. Starting with the desktop, migrating from proprietary office productivity suites to LibreOffice is described by concerned interviewees as a difficult task that should be left for later stages. Rationales referenced include the potential clash with expectations, comfortness, and resistance-to-change among end-users aligning with other observations (Digitaliseringsstyrelsen, 2025). It should be noted, however, that several interviewees report on opposing experiences, highlighting office suite migration as manageable and valuable first step.

In the following phase, the change process can start by addressing modules where migration requires considerably more effort, but is motivated by financial incentives or key policy goals, e.g., addressing critical "sovereignty gaps" in the digital infrastructure. A challenge for migration efforts in this phase is that there is typically no funding available, and loans cannot be considered (låneloft). Hence, efforts should start where there is a business case (beyond sovereignty) to build a frame of reference and understanding of the softer benefits (e.g., sovereignty).

6.3.3.3 Front- and mid-layer migration for user-facing impact

The third approach focuses on the more user-facing parts of the IT stack, aiming for impact while investments and risk may be higher. In Denmark, multiple initiatives are currently working in parallel within this approach.

On the national level, the Agency for Governmental IT Services (Statens IT) is currently developing (on the request of the Danish Road-Traffic Authorities[26]) an OSS desktop solution (SIA Open) covering the whole desktop environment (Sørensen 2025). This also includes collaboration and productivity environment covered by solutions such as OpenDesk[27], MijnBureau[28], and La Suite Numerique[29], developed by the German, Dutch and French governments respectively, now also evolving to a EU level collaboration through the European Digital Infrastructure Consortium for Digital Commons (EDIC-DC)[30].

The Danish desktop solution will be Linux-based and enable full remote administration as regular proprietary environments. After introducing a Linux-based desktop client with management and basic services, the plan is to add additional services for printers, file sharing, and desktop applications, such as OpenDesk and La Suite Numerique, and

[24] https://statens-it.dk
[25] https://www.domstol.dk
[26] https://www.danishroadtrafficauthority.dk/
[27] https://www.opendesk.eu/en
[28] https://minbzk.github.io/mijn-bureau-infra/
[29] https://lasuite.numerique.gouv.fr/
[30] https://digital-strategy.ec.europa.eu/en/news/commission-launch-digital-commons-edic-support-sovereign-european-digital-infrastructure-and

to improve integrations with non-European incumbent infrastructure. It is important to note, however, that European corresponding projects are emerging. In Germany, e.g., both the federal government and the state of Schleswig-Holstein are investigating expanding the scope of a fully sovereign workspace. Again, this highlights the importance of national and local initiatives in Denmark to maintain cross-border connections and awareness, avoiding duplication of efforts.

In parallel and at the municipal level, OS2 is working to initiate, advance, and merge three related projects: OS2borgerPC, OS2skole, and OS2adm, all full Linux-based operating systems with relevant software and applications intended for public spaces, schools, and civil servant use cases. While the projects are at different levels of maturity and completeness, together they serve as a foundation towards creating a sovereign desktop solution in line with SIA Open. Further, there are ongoing developments among service suppliers, e.g., regarding OS2borgerPC, also aimed at creating a sovereign desktop solution.

6.3.4 Joint agreements and coordinated rollouts

Joint agreements and "bølgeplaner", i.e., centrally coordinated, phased roll-out plans for IT solutions across PSOs, are requested by several interviewees for the introduction of key OSS solutions for strategic areas. Such roll-outs would help align government IT with broader policy goals, e.g., in terms of digital sovereignty.

Interviewees accordingly request a stricter, clearer directive and strategy from the top down to scale initiatives, e.g., to grow sovereignty and control over public-sector IT. Scale is typically required to achieve significant impact, efficiencies, and sustainability, which is why the stick can sometimes be more useful than the carrot, as one interviewee put it.

In Schleswig-Holstein, the regional authorities drive development through internal resources, in collaboration with the regional public service provider Dataport, and several European third-party vendors. The centralisation enables the coordinated, structured rollout of the new services, one piece and step at a time, a process that has been ongoing for several years and has not resulted in the reduction of 80% of licences to a non-European incumbent, who has otherwise dominated the region. By 2029, the rollout is expected to have reduced by 99%.

The central development and standardisation of common infrastructure and systems, such as the joint design system for public digital services developed by the Government Digital Services (GDS) in the UK, represent another top-down approach to coordinated rollout. In Kenya and Trinidad and Tobago, a phased transformation is planned, starting with early pilots and later transcending across national ministries.

6.3.5 Designing standards and reference implementations for sovereign digital infrastructure

Governments can accelerate digital transformation by defining common standards and providing reference implementations that guide how public-sector digital infrastructure should be built. This approach helps reduce fragmentation, enables interoperability across PSOs, and supports long-term digital sovereignty by anchoring solutions in

open, reusable and transparent technical foundations. It allows PSOs and suppliers to build against clearly specified interfaces rather than reinventing components or relying on proprietary stacks.

Germany's emerging Deutschland-Stack provides a useful example of this strategy. It aims to create a sovereign, interoperable and European-aligned technology platform, built on open standards and modular OSS base components that can be reused across federal, state and municipal levels. The initiative defines a layered model of technologies and standards, published through an official portal and refined through iterative public consultations, positioning the stack as a unified reference architecture and implementation pathway for digital services. Its goal is to offer concrete, reusable elements that enable consistent service delivery and strengthen digital sovereignty.

For Denmark, similar efforts would mean publishing national interface standards, curating reference components built on open standards, and aligning with established international frameworks such as GovStack, which provides global reference architectures and reusable digital building blocks. Such an approach, as also adopted by the Irish government, can help ensure coherence across PSOs, reduce integration barriers, and create a shared technical foundation that supports sovereign, interoperable digital public services.

6.3.6 Dual-channel adoption strategies

Completely replacing proprietary software may not always be realistic or necessary, while many of the benefits from OSS can still be gained. By creating and adopting viable OSS options, the dependency on single service suppliers is reduced, and by extension, pivots control and power from the supplier to the PSOs (Linåker & Regnell, 2020). This includes leveraging bargaining power over licensing costs while also building resiliency, e.g., in terms of digital sovereignty, should there be a need to switch to alternative solutions.

This form of dual-channel strategy has been reported by both interviewees at the local and regional government levels, where LibreOffice was used as an office productivity solution for several years. Yet, in both cases, they report how the benefits ended simultaneously as their respective organisations signed framework agreements with a leading non-European supplier of incumbent office productivity suites. The rationale for the transition is described as management's general quest to streamline the solutions used by other PSOs, although there was no technical or usability rationale underpinning the decision.

6.4 Capability to provide and coordinate shared open source collaboration infrastructure

Summary

For OSS adoption and collaboration to scale across the public sector, PSOs need reliable, common infrastructures for sharing, reusing and co-developing software. Our investigation shows that today these infrastructures are fragmented, often reliant on commercial platforms outside European jurisdiction, and inconsistently maintained. This creates barriers to reuse, limits transparency, and undermines ambitions for digital sovereignty.

Specifically, we find in the context of providing and coordinating shared OSS collaboration infrastructure that public-sector OSPOs should consider:

- establishing and governing a government social code collaboration platform, enabling PSOs to share code, documentation and architectural artefacts in a secure, sovereign environment that supports both open and inner source collaboration.
- supporting standardised tooling and templates on the platform, including metadata requirements, documentation guidelines, continuous integration pipelines and quality checks that lower the threshold for reuse and improve findability.
- developing and maintaining a national OSS solution catalogue, aligned with international metadata standards (public-code.yml), to help PSOs identify existing solutions, compare alternatives and build on shared components rather than procuring or developing in isolation.
- coordinating taxonomy, mapping and categorisation practices across government so that listed solutions correspond to how PSOs structure their procurement and portfolio management in practice.
- building communities of practice around both the platform and the catalogue, involving PSOs, suppliers and non-profit actors to improve data quality, evaluate alternatives and share operational experience.
- aligning national infrastructures with European initiatives, ensuring federation with other public platforms and compliance with emerging interoperability requirements to maximise cross-border reuse and avoid fragmentation.

Below, we expand on the infrastructure components required and how OSPOs can support their establishment, governance and long-term maintenance.

6.4.1 Government social code collaboration platform

A common social code collaboration platform would provide a joint infrastructure, enabling sharing and reuse on the one hand, and open collaborative development on the other. Architectural blueprints, documentation, and risk analysis are other types of artefacts that could be shared on such a platform, with some parts open and others kept closed to the public sector only. The platform would, hence, be an enabler both for open and inner source collaboration.

The current use of GitHub among many PSOs raises concerns about data and sovereignty, inhibiting the use and sharing of solutions on the otherwise widely recognised platform. One interviewee adds the need for a platform where developers can easily share and reuse technical components. Support and templates for sharing documentation and metadata should be provided to lower the bar, improve quality and findability. Responsibility for the platform could be tied to the national government OSPO and integrated with aligned responsibilities.

The German Centre for Digital Sovereignty (ZenDIS) provides an example with its openCode platform[31], which is a GitLab-based OSS social-coding platform. The platform is intended for federal, state, and local government PSOs, providing a central place for them to publish, share, and jointly develop public-sector OSS projects, with the aim of avoiding parallel development and strengthening digital sovereignty in government IT. The platform functions both as a software directory and a collaborative development environment, including quality checks and badges for aspects such as openness, maintenance, use, and security to support reuse in procurement and projects. As of the latest public figures, it hosts several thousand registered users and a few thousand projects, and has been expanding quickly.

In the Netherlands, the government is considering adopting Forgejo[32] as their national social code collaboration platform. Forgejo is a community-governed, self-hosted Git forge that began as a fork of Gitea and is stewarded by the non-profit Codeberg e.V.[33], aiming to provide a fully free, federated alternative to proprietary platforms. Codeberg is a large public Forgejo instance run by that non-profit, offering Git hosting, issue tracking, CI and pages as a privacy-friendly alternative to GitHub.

Inspired by German and Dutch examples, the Swedish government recently released a report proposing a similar national social code collaboration platform so that public-sector bodies can share, reuse, and co-develop OSS rather than build similar solutions in isolation (DIGG – Myndigheten för digital förvaltning, 2025). The report highlights several current challenges, including fragmented code sharing, ad-hoc GitHub use, and a lack of clear governance, which currently hinder systematic reuse, efficiency, and digital sovereignty. The proposed platform would offer repositories, documentation, issue tracking, and templates, along with guidance from a National Government OSPO, which is implicitly part of the report's several recommendations.

[31] https://opencode.de/en
[32] https://forgejo.org
[33] https://codeberg.org

The OSPO would further support by developing and providing training on governance models, contribution rules, and legal support to handle licensing, procurement, and security. The report further emphasises that the platform should complement, not replace, existing open ecosystems by federating with other public platforms and aligning with European interoperability and OSS initiatives, and concludes that such a platform is strategically important to meet Sweden's digitalisation goals and avoid further fragmentation and vendor lock-in.

6.4.2 Government open source solution catalogue

There also needs to be clarity on which existing OSS solutions or configurations thereof address the various needs of PSOs. Creating a searchable catalogue highlighting existing solutions is commonly occurring across countries (Linåker & Muto, 2024). In Spain, the use of the national catalogue is mandated by law, requiring all PSOs to publish the applications they acquire to enable reuse by other PSOs. Source code, documentation, license conditions, and associated costs should be shared and declared. While the Spanish catalogue is closed to PSOs only and not limited to OSS, the French counterpart, code.gouve.fr, is publicly open and explicitly focuses on OSS used and/or developed by French PSOs. The catalogue is maintained by the National Government OSPO, which is constituted by the Free Software Unit within DINUM.

All OSS listed in the catalogue have adopted the public-code.yml metadata standard for public-sector OSS projects, which facilitates findability and adoption. By including the metadata file in the catalogue of an OSS project, it can be queried and included in other catalogues, enabling interoperability among regional, national, and international catalogues and further promoting reuse. Other countries, such as Italy and the Netherlands, have also adopted the standard, improving cross-border reuse and adoption of OSS projects. The recently launched European OSS solutions catalogue aggregates and presents an overview of public-sector OSS solutions across national solution catalogues, based on the public-code.yml metadata.

Categories and indexing used across the catalogues, however, do not always match those commonly used in practice across PSOs. Mapping such solutions and configurations to Gartner's 16 types of standard software, which is used as a reference in SKI's framework agreements, is proposed to provide additional clarity. Such mapping could also extend to and cover other dimensions and use cases relevant to PSOs across different levels of government. The investigation should also work analytically and in collaboration with PSOs to identify best-in-class OSS alternatives, adding references and user feedback to help PSOs navigate and evaluate options.

The mapping should ideally be developed and maintained collectively through an open community of practice across government, and should also include suppliers and other sectors that may provide valuable information on potential alternatives. To further reduce knowledge barriers, each solution or configuration may include details on PSOs, suppliers, and non-profit organisations that can support in the evaluation and acquisition process. The catalogue may, per one interviewee, also want to consider including non-OSS solutions that, in other ways, meet a certain set of requirements, e.g., by using open standards and enabling easy replacement and operation in alignment with EU Data legislation. In the end, PSOs are less interested in whether a solution is OSS than in whether it solves the problem.

Historically, the national software catalogue Softwarebørsen.dk served as an important resource by indexing software applications used and of interest to the Danish PSOs (Open Source Observatory and Repository, 2012). The catalogue was a collaboration between the National Knowledge Centre for Software and the vendor ecosystem in Denmark.

Today, a wider-purpose Digitalisation catalogue platform Digitaliseringskataloget, is available, although mainly focused on indexing services that are part of the common national digital infrastructure used by all 98 municipalities (KOMBIT, n.d.). The platform provides an overview of both software in the common public-sector infrastructure and its different parts, as well as documentation and knowledge related to the infrastructure.

Another, though narrower, software catalogue is that of OS2, listing the 25+ OSS projects developed and maintained by the association (OS2, n.d.). The projects are in turn mainly hosted on GitHub, which also hosts seven PSOs identified as government institutions, including the Royal Library, the National Tax Administration, and the National Museum of Denmark (GitHub, n.d.)

6.5 Capability to manage open source licence selection and compliance

Summary

Licence compliance remains uneven across the public sector. Many PSOs lack the legal and technical expertise needed to assess licensing obligations for both inbound and outbound OSS, which creates uncertainty and risk in procurement, development and release processes. Public-sector OSPOs therefore play an important role in building consistent routines, shared resources and governance mechanisms for compliant and responsible OSS use.

Specifically, we find in the context of managing OSS licence selection and compliance that public-sector OSPOs should consider:

- developing and maintaining curated licence lists and policy guidance, offering clear recommendations on suitable licences and helping PSOs navigate differences between permissive, copyleft and other licence families.
- embedding compliance checks in intake processes, ensuring early evaluation of licence terms, compatibility and obligations before OSS components are embedded in production systems.
- promoting SBOM-based compliance monitoring, enabling transparency over dependencies, facilitating automated checks and supporting continuous oversight rather than ad-hoc reviews.
- conducting pre-release IP and licence verification, reviewing codebases, attribution, documentation and compatibility to ensure that releases meet legal and policy requirements.
- supporting periodic audits and inventory management, helping organisations maintain up-to-date overviews of licences, dependencies and associated risks.
- integrating licence compliance into procurement, providing training, templates and support so procurement officers can evaluate OSS options, anticipate obligations and include appropriate terms in contracts.
- factoring AI-assisted code generation into compliance routines, ensuring that intake, SBOM-based monitoring, and pre-release verification account for code partly or wholly generated by AI tools, including checks on model licences, data provenance, attribution requirements, and risks of inadvertently introducing restricted or copyrighted material.

Below, we outline the mechanisms through which OSPOs can support this work and the practices that help sustain consistent, organisation-wide compliance.

6.5.1 Curated licence lists and policy guidance

A common compliance mechanism is the development of curated lists of recommended and discouraged licences, maintained and updated in response to organisational needs and queries. These lists provide PSOs with clear guidance on which licences are suitable for use and under what conditions, and are often complemented by broader procurement guidelines explaining distinctions between permissive, copyleft, and other licence families.

For example, the German Centre for Digital Sovereignty (ZenDiS) maintains an evolving list of recognised OSS licences that is updated as PSOs raise new questions about reuse or inbound contributions. Similarly, Developers Italia, the National Government OSPO of Italy, has issued explicit legal guidance in its procurement materials, clarifying the implications of different licence families for both reuse and release. At the local level, the City of Ventspils uses a preferred-licence approach, recommending the EUPL due to its availability in Latvian and suitability for public-sector reuse. These curatorial functions allow PSOs to make informed decisions without requiring each team to interpret complex licence texts independently.

6.5.2 Embedded compliance in intake rocesses

Intake processes for evaluating OSS components frequently embed licence-compliance checks. These processes may include initial review of licence terms, compatibility evaluation with organisational policies, and verification of how obligations (e.g., attribution, disclosure, reciprocity) would apply when reused or redistributed. Such mechanisms ensure that licence risks are identified early, before components become deeply embedded in production systems.

Institution-centric OSPOs illustrate this approach most clearly among reported cases of public-sector OSPOs (Linåker et al., 2024). At the European Commission's OSPO, intake processes involve vulnerability and licence-health assessments before components may be used, providing traceability and documented justification for approval. Within the Dutch Tax and Customs Administration, developers may autonomously select OSS components, but their choices are validated through lightweight processes that include licence-compatibility reviews supported by a virtual compliance team. These cases demonstrate that embedded intake processes can balance developer autonomy with institutional risk management.

6.5.3 SBOM-based compliance monitoring

There is growing use of Software Bills of Materials (SBOMs) as a practical tool for license-related oversight. SBOMs enable OSPOs to map all third-party components used in a project, identify their licenses, detect incompatible or problematic dependencies early, and facilitate automated or semi-automated checks before release.

As an example, the German Centre of Digital Sovereignty (ZenDIS) automatically renders and requires SBOMs for all software listed in the national catalogue (OpenCode), supporting automated security and licence checks. At the European

Commission, SBOMs are used to track the licence profiles of individual projects prior to external release, although this is not yet done across the full dependency graph.

While SBOM-driven compliance is not yet uniformly implemented, it signals a shift from ad hoc reviews toward continuous monitoring.

6.5.4 Pre-release IP and licence verification

Before software is released as OSS, OSPOs commonly conduct internal intellectual-property and licence-compliance checks. These may involve scanning the codebase for embedded third-party licences, reviewing documentation and attribution, ensuring that disclosure requirements are met, and validating consistency between dependency licences and the intended outbound licence.

For example, at the European Commission, outbound releases are contingent on both an IP review and a dependency-licence assessment conducted by the OSPO and its legal counterparts. The French Public Employment Service has a formalised cross-departmental review group that provides similar oversight, bringing together legal, security, and technical experts. In Local government, the City of Paris performs targeted licence checks before releasing components of its Lutece platform to ensure permissive licensing remains appropriate for its dissemination strategy.

These checks serve as safeguards against inadvertent violations and help ensure that public releases comply with legal and policy requirements.

6.5.5 Periodic audits and software inventory management

Some organisations conduct regular audits of their software inventories to assess the licences associated with in-use components, identify outdated or vulnerable dependencies, and address risks proactively. Such audits may alternate between internal and external assessors, providing both institutional continuity and independent verification.

For instance, the City of Ventspils performs annual licence and dependency audits, alternating between internal and external auditors. The City of Paris maintains a detailed inventory of OSS components, including versions, dependencies, and architectural relationships, that enables rapid impact assessment when license- or security-related issues emerge. These practices illustrate how inventory management can sustain organisational compliance in environments characterised by evolving software landscapes.

6.5.6 Procurement-integrated licence compliance

Procurement is another critical point for licence compliance. Training and detailed procurement guidance help officers evaluate OSS options during procurement workflows, anticipate licence obligations, and include requirements for outbound release in contracts. Where external development is procured, OSPOs help ensure that vendors adhere to open-source-compatible development practices and avoid lock-ins.

Several of the surveyed public-sector OSPOs provide detailed procurement templates and support to ensure licence compliance and encourage OSS consideration in line with

national or regional policies. In the City of Bratislava, its OSPO embeds OSS requirements into tender specifications for new systems to facilitate later reuse or release. Association-based OSPOs such as OS2 and VNG also provide procurement frameworks for member municipalities, including standard clauses ensuring that collaboratively developed software remains openly licensed.

6.5.7 Compliance considerations for AI-assisted code generation

AI-assisted development tools are becoming increasingly used in software development accelerating speed across the software development life-cycle. One interviewee considers it necessary to reassess which governance structures that are needed around code and the resources working with and around software delivery. This especially includes the compliance perspective, where OSPOs must ensure that compliance routines account for code whose provenance is partially or wholly machine-generated.

AI outputs may embed licensing obligations originating from training data or reproduce copyrighted material, making it essential to document when and how AI agents are used during development. Intake processes should therefore include basic checks on model licences, data provenance, and potential attribution requirements, while SBOM-based monitoring should be extended to flag components created through AI assistance.

Pre-release verification must also address AI-generated artefacts by ensuring that no restricted or unlicensed material is inadvertently introduced, and that relevant documentation is included in release reviews. By integrating these considerations into existing routines for OSS intake, SBOM-production, pre-release checks, and audits, OSPOs can maintain legal clarity and reduce risk as AI-assisted development becomes a routine part of the software supply chain.

6.6 Capability to steward public-sector open source projects

Summary

Sustainable OSS adoption in the public sector requires clear stewardship. OSS projects must have actors who take responsibility for governance, coordination, community development and long-term maintenance. Our investigation shows that stewardship capacity varies widely across PSOs and countries, and that different models are needed depending on context, maturity and resource levels.

Specifically, we find in the context of stewarding public-sector OSS projects that public-sector OSPOs should consider:

- supporting association-based stewardship models, where neutral, member-driven organisations provide governance structures, pooled resources and continuity. These models lower barriers for collaboration, especially among municipalities with limited capacity.
- enabling supplier-led stewardship where appropriate, ensuring that service providers who develop and maintain OSS solutions also uphold open governance, quality, and community practices, while PSOs retain the capability to validate deliverables and avoid new forms of lock-in.
- strengthening government-internal stewardship models for PSOs with sufficient capability, allowing public organisations to own and coordinate development directly, build internal competence and reduce long-term dependency on external vendors.
- developing stewardship roles within state-owned service providers, ensuring they can host, adapt and deliver OSS solutions while maintaining openness, transparency and shared governance with PSOs rather than defaulting to closed operational routines.

Below, we describe how these stewardship-models function in practice and the capabilities required for their long-term sustainability.

6.6.1 Association-based stewardship models

Association-based stewardship is common across Europe and represents one of the most mature and scalable stewardship models for public-sector OSS. Member-driven, neutral, non-profit organisations, typically composed of municipalities and regions, act as stewarding bodies for a portfolio of shared digital solutions. These associations provide the administrative, legal, and governance backbone needed for long-term collaboration.

In Denmark, OS2 exemplifies this model. With 80+ of 98 municipalities as members, OS2 hosts more than 25 OSS projects and provides a structured framework for starting new projects, maintaining existing ones, and coordinating shared needs. Similar models appear across Europe, including VNG (Netherlands), Sambruk (Sweden), Adullact (France), and Open Cities (the Czech Republic). These organisations exemplify how public-sector collaborations around OSS depend on a neutral steward capable of maintaining community trust, managing governance structures, and coordinating development across multiple jurisdictions. Associations reduce dependency on individual champion municipalities by providing continuity and pooling resources, capabilities, and risks among many public actors.

By offering shared governance, legal structures, and project management capacity, associations lower the barriers for PSOs, especially smaller municipalities, to participate in collaborative development. They also support sustainability through cost-sharing arrangements, collectively funded maintenance, and the establishment of consistent development practices across member organisations.

6.6.2 Supplier-led stewardship models

Service suppliers also commonly act as stewards, particularly when they both develop and maintain OSS projects. Their stewardship typically aligns with a service-based business model in which suppliers provide development capacity, maintenance, hosting, and support services while keeping the core solution open and reusable. In Denmark, Magenta's stewardship of OSDataScanner[34] illustrates this model, while hybrid setups can also include both service suppliers and PSOs.

Suppliers provide critical support to public entities, especially at the local government level, where internal technical capabilities are often limited. They contribute throughout the solution lifecycle from planning and acquisition to implementation and operational support. Their stewardship extends to ensuring technical continuity, securing project quality, and responding to evolving requirements.

Effective supplier stewardship requires PSOs to maintain strong internal capabilities in requirements engineering, validation, and procurement. While suppliers can assist, PSOs must define requirements, review deliverables, and ensure OSS licensing and governance requirements are met. Healthy supplier ecosystems are essential for OSS sustainability; suppliers act as custodians of technical expertise and operational capacity, particularly when public entities lack the internal capacity to scale.

6.6.3 Government-internal stewardship models

A growing number of resourceful PSOs, including national administrations and larger municipalities, are moving toward internal stewardship models, in which the public entity itself owns and maintains the solution. Instead of procuring end-to-end services, these organisations procure development resources that work alongside internal teams. Consultants are embedded temporarily, contributing to development efforts before handing over ownership and operational responsibility to the public entity.

[34] https://www.magenta.dk/en/solutions/osdatascanner-en/

This model provides flexibility and control over technical decisions, aligns solutions more closely with internal requirements, and creates opportunities to share and reuse components across other PSOs. By retaining ownership, public organisations ensure long-term alignment with policy objectives, reduce lock-in risks, and strengthen internal digital capabilities. The German Centre of Digital Sovereignty (ZenDIS) exemplifies the model through the development of their OSS-based office productivity suite OpenDesk.

When a capable public entity, such as the Danish Court Administration (Domstolsstyrelsen), assumes stewardship, it can coordinate development not only for itself but also for other PSOs, ensuring shared benefits and avoiding duplication of effort. Further, by bringing together larger PSOs such as KOMBIT, DBC Digital, Agency for Governmental IT Services (Statens IT), and Danish Court Administration (Domstolsstyrelsen), these PSOs can pool resources, enabling more substantial joint investments that support both capable and less-resourced PSOs.

A risk is that as an OSS project grows in adoption, the maintenance burden will increase, as will the inflow of requests that are not aligned with the stewarding PSO's priorities. The Signalen project, stewarded by the City of Amsterdam, provides one such example. In this case, the city and its partners are seeking to transfer the project to VNG's stewardship, though it is a lengthy and complex process. PSOs should therefore consider the long-term stewardship of their projects from the start, and whether their own organisations are committed to this task or whether it is better managed elsewhere.

6.6.4 State-owned service-provider stewardship models

State-owned service providers represent another important stewardship model. These entities sit between government and market suppliers, providing stable operational capacity and long-term service delivery while aligning with public-sector values such as transparency, sovereignty, and shared control.

OperatorICT[35] in the City of Prague, iMio[36] in the context of the Walloon municipalities, pagoPA[37] in Italy, and Agency for Governmental IT Services (Statens IT) provides some examples of the model, the latter through its work on the SIA Open project. While Agency for Governmental IT Services does not typically develop new software, it takes existing OSS solutions, customises them, and delivers them as a service to clients.

This inbound-focused model positions the state-owned provider as a potential steward. Still, interviewees highlight that capabilities for facilitating governance and open collaboration are still missing - an issue also reported by public-sector OSPO interviewees in regard to national and regional service providers in Germany and the Netherlands.

[35] https://operatorict.cz/en
[36] https://smartweb.imio.be/en/home
[37] https://www.pagopa.gov.it/

6.7 Capability to measure, analyse, and follow up on open source activities

Summary

Systematic measurement and follow-up are essential for understanding whether OSS strategies, investments and support efforts produce meaningful outcomes. Our investigation shows that such practices remain limited across many PSOs due to resource constraints, decentralised processes and the absence of shared frameworks. Public-sector OSPOs therefore need the capability to collect, analyse and act on data that improves decision-making, strengthens governance and aligns practice with policy goals.

Specifically, we find in the context of measuring and analysing OSS activities that public-sector OSPOs should consider:

- demonstrating value and securing long-term support, using indicators such as participation levels, published projects and collaboration activity to communicate progress and justify continued investment.
- supporting operational oversight and risk management, tracking how intake and release processes function, monitoring compliance routines such as licensing reviews and SBOM scanning, and identifying bottlenecks that require intervention.
- informing platform, project and service improvement, monitoring usage patterns, contribution trends and user satisfaction to guide enhancements to catalogues, social code collaboration platforms and shared OSS solutions.
- strengthening sustainability and project-health monitoring, observing governance practices, contributor engagement and maintenance distribution across organisations to ensure ongoing viability of shared projects.
- enabling learning, capability-building and needs identification, collecting data on training needs, process challenges and cultural readiness to direct targeted support.
- feeding evidence back into strategy and policy, using aggregated insights from adoption, release and contribution patterns to refine OSS strategies, update guidance and prioritise workstreams.

Below, we expand on the measurement practices, indicators and feedback loops that support effective oversight and continuous improvement across the public-sector OSS

6.7.1 Demonstrating value and securing long-term support

A recurrent rationale for measurement is the need to evidence the value of OSS work, both to internal leadership and to policymakers who allocate resources. OSPOs use various indicators to demonstrate uptake and activity, such as growth in the number of participating public administrations, increases in published OSS projects, and visible collaboration across repositories and platforms.

In several National government cases, such as Italy and Germany (Linåker et al., 2024), OSPOs routinely track metrics such as the number of organisations registered in their catalogues and the volume of published projects, using these data points to articulate the reach and momentum of national OSS policy. By contrast, the French National Government OSPO (DINUM) reports that resource limitations hinder systematic measurement, making it difficult to demonstrate the scope of public-sector engagement and to advocate for long-term operational funding. These examples highlight the risks of inadequate measurement, as the absence of evidence can limit institutional willingness to sustain investment.

6.7.2 Operational oversight and risk management

Another rationale for follow-up relates to operational oversight. OSPOs apply measurement to understand which components and projects are being used and by whom, how OSS intake and release processes are functioning, and whether compliance checks (e.g., licensing reviews, SBOM-based scanning) are consistently completed.

For instance, the European Commission's OSPO monitors the use of its intake process, including the volume of components undergoing vulnerability and licence-health assessments. These indicators help identify bottlenecks in intake workflows and ensure compliance with internal security and IP procedures before release. Similarly, the Dutch Tax and Customs Administration uses project-level SBOM data to maintain visibility into dependency licensing and the status of release reviews. Public-sector OSPOs thus leverage measurement to reduce operational risk and ensure controlled development and release practices.

6.7.3 Platform, project, and service improvement

OSPOs also measure activity to inform ongoing improvement of the platforms and OSS projects they steward. Usage statistics, contribution activity, and participation trends reveal which projects are thriving, where additional support or coordination may be needed, and whether shared infrastructures such as national catalogues or social code collaboration platforms meet user needs.

In Italy and Germany (Linåker et al., 2024), for example, monitoring the number of projects published to national catalogues and activity levels within their social code collaboration platforms helps determine how well these infrastructures serve PSOs and where enhancements may be required. In local government settings, measurement can also extend to end-user outcomes. The City of Bratislava, for instance, tracks user-satisfaction indicators for its OSS-based e-services, using resident feedback to iteratively adjust features and improve service quality. These forms of follow-up help

ensure that technical platforms evolve in line with user expectations and organisational needs.

6.7.4 Sustainability and project health monitoring

Where OSS projects are co-developed across multiple organisations, metrics support stewardship and sustainability. OSPOs observe contributor participation, responsiveness to issues, and the functioning of project governance structures to ensure long-term viability.

Association-based OSPOs exemplify this dynamic. OS2 (Denmark) and VNG (Netherlands) monitor participation levels across municipalities, the distribution of maintenance responsibilities, and vendor involvement in their shared projects. Tracking these indicators helps them identify when certain projects require additional investment, governance adjustments, or renewed community engagement. Similarly, the City of Paris follows contribution patterns to the Lutece platform to prioritise feature development and community-building efforts. These measurements help sustain cooperative development models over time.

6.7.5 Learning, capability-building, and needs identification

Measurement also supports organisational learning and capability-building. Through surveys, informal observation, and process-level data, OSPOs identify where staff encounter barriers, what training topics require additional attention, and how internal culture is evolving.

For example, the Lero Academic OSPO used an internal survey to identify researcher pain points in OSS licensing and tooling, which informed new mentorship and workshop initiatives. Similarly, intake-process data at the European Commission reveals which departments encounter repeated challenges, prompting targeted support or refinement of documentation. These feedback loops allow OSPOs to adapt their support functions to practitioner needs and to strengthen institutional competence.

6.7.6 Feedback loops to strategy and policy

Finally, follow-up provides OSPOs with insights that inform strategy and policy refinement. By observing adoption patterns, monitoring areas of friction, and identifying where guidance is least understood or applied, OSPOs can assess whether existing OSS strategies are being implemented effectively.

For instance, recurring bottlenecks identified in Germany's SBOM-based catalogue submissions help highlight where national policy ambitions, such as "open-by-default" development, encounter practical difficulties. At the European Commission, aggregated indicators from intake, release, and contribution activities inform periodic updates to the Commission-wide OSS strategy and shape the priorities of training programmes. These feedback loops allow OSPOs to translate operational evidence into policy-level recommendations, ensuring closer alignment between strategic goals and everyday practice.

6.8 Capability to enable Inner Source collaboration

Summary

Many PSOs face situations where full OSS release is not yet possible, even though collaboration would still be valuable. Inner Source offers a practical intermediate approach by applying OSS-like development methods inside or across PSOs, allowing code sharing, reuse and joint problem-solving before external publication is appropriate. Our investigation shows that Inner Source can strengthen consistency, reduce duplication and build the cultural and technical foundations needed for open-by-default practices.

Specifically, we find in the context of enabling Inner Source collaboration that public-sector OSPOs should consider:

- supporting Inner Source for intra-governmental collaboration, enabling PSOs to share code, prototypes, documentation and risk assessments internally when external release is not yet feasible due to sensitivity, immaturity or contractual constraints.
- reinforcing open-by-default as the preferred development practice, while recognising the situations where temporary internal development is justified and ensuring that Inner Source remains a bridge rather than an endpoint.
- using Inner Source as an on-ramp to open practice, helping teams gain experience with shared repositories, code review, issue tracking and modular development before navigating full compliance, security and quality requirements for public release.
- leveraging government social-code collaboration platforms as enablers, providing shared infrastructure for repositories, templates, documentation and compliance artefacts that support consistent practices across departments and agencies.

Below, we describe how Inner Source functions in the public sector, when it is most appropriate, and how OSPOs can support its adoption and governance.

6.8.1 Inner Source for intra-governmental collaboration

Inner Source is commonly framed as the application of OSS development practices within an organisation. From a public-sector perspective, however, the concept can also extend across PSOs, enabling collaborative development while not yet working in the full open under OSS licences. This form of collaboration allows PSOs to share knowledge, coordinate development efforts, and reuse components that may not be suitable or permissible for public release. Artefacts such as internal documentation,

preliminary risk assessments, early-stage prototypes, or partially developed code can circulate internally across agencies, offering transparency and reuse benefits that external publication cannot yet achieve.

Examples of this dynamic are visible in several institution-centric OSPOs (Linåker et al., 2024). At the European Commission, the internal social code collaboration platform enables staff across Directorates to access, review, and contribute to each other's repositories before any decision to publish code externally. Similarly, within the French Public Employment Service, development teams operate with a high degree of transparency toward each other, sharing code and design artefacts internally even when contractual considerations or security sensitivities delay external release. Across these cases, reports describe Inner Source as a practical mechanism for lowering barriers to collaboration and fostering consistency across organisational boundaries, particularly when different PSOs face similar challenges but cannot immediately release their solutions as OSS.

6.8.2 Open-by-default as preferred development practice

Despite its usefulness, many public-sector OSPOs emphasise that open-by-default development is the preferred practice (Linåker et al., 2024). Publishing code directly as OSS avoids duplicating intake and release processes, ensures traceability, and enables PSOs to benefit from the broader advantages of openness, such as transparency, vendor neutrality, and access to external contributions.

However, several interviewees highlighted scenarios that justify temporarily keeping work internal. These include sensitive security contexts, immature software that may mislead or be misused if released prematurely, or contractual conditions involving suppliers or proprietary components. In these cases, Inner Source serves as an intermediate model that respects organisational constraints while retaining the collaborative advantages of OSS-like practices.

6.8.3 Inner Source as an on-ramp to open practice

Inner Source also plays a transitional role by building internal capability and confidence before moving to full OSS release. By enabling teams to work through shared repositories, open issue tracking, code review, and modular development internally, PSOs can cultivate the cultural and procedural foundations needed for sustainable OSS participation.

This on-ramp function is particularly relevant in institution-centric OSPOs (Linåker et al., 2024). At the Dutch Tax and Customs Administration, for example, teams routinely share code internally through centralised tooling, enabling developers to gain experience with open workflows while internal compliance and security checks are completed. At the European Commission, Inner Source practices help identify which projects are mature enough for release and guide developers through the adaptation needed for community-ready publication. These cases demonstrate how Inner Source can help normalise open collaboration in organisations where developers have autonomy but still require structured support to navigate risk, compliance, and quality expectations.

6.8.4 Social code collaboration platforms as Inner Source enablers

Both interviewees and reports (Linåker et al., 2024) highlight the importance of government social code collaboration platforms as enablers of both open and Inner Source practices. Such platforms provide PSOs with a shared infrastructure for collaboration, publishing, and exchanging artefacts, helping align development practices across diverse agencies. They typically host repositories, documentation, templates, compliance artefacts, and communication channels, making them foundational for intra-governmental collaboration, whether or not repositories are publicly visible.

Institution-centric OSPOs, such as the European Commission's and the Dutch Tax and Customs Administration's platforms, are both highlighted as enablers for their respective Inner Source practices. The platforms allow developers across departments and units to access, review, and contribute to one another's codebases using OSS-like workflows, even before legal or security clearance for external publication. The reports describe how such infrastructures foster early visibility into ongoing work, reduce duplication across teams, and support cross-organisational problem-solving, while also providing structured spaces for documentation, templates, CI pipelines, and compliance artefacts. In this way, the platforms not only facilitate internal collaboration but also serve as preparatory environments that help teams develop the routines and confidence needed for eventual open-by-default development.

6.9 Capability to drive advocacy and build open source communities

Summary

Cultural factors remain some of the most persistent barriers to OSS adoption in the public sector. Misconceptions, risk aversion and unfamiliarity with open practices slow progress even when policy and technical conditions are favourable. Public-sector OSPOs therefore play an important role in advocacy and community-building to help shift norms, reduce perceived risks and create the social infrastructure required for sustained collaboration.

Specifically, we find in the context of advocacy and community-building that public-sector OSPOs should consider:

- cultivating communities of practice, creating spaces where engineers and practitioners can meet, share experiences and coordinate work across organisational boundaries. These communities help surface common needs, reduce duplication and build a shared identity around public-sector OSS practice.
- establishing multi-stakeholder advisory structures, enabling structured dialogue between government, suppliers, civil society and the wider OSS ecosystem to inform decision-making and strengthen legitimacy.
- supporting cross-government and cross-border collaboration, connecting PSOs with peers in other municipalities, regions and countries to exchange tools, practices and lessons learned, and to accelerate adoption through shared experience.
- leading advocacy for cultural and organisational change, building trust, reducing perceived risk and helping stakeholders understand OSS as both a technical and strategic instrument. This includes communication work, awareness-raising, training, and providing clear narratives that link OSS to goals such as sovereignty and resilience.

Below we expand on how OSPOs support these forms of engagement and why they are essential for scaling OSS adoption in the public sector.

6.9.1 Communities of practice

Growing inter-organisational communities is a good way to coordinate on new and existing projects to promote sustainable and well-maintained solutions. It can also be an arena for identifying new projects and common use cases. Joint conferences and touchpoints can serve as facilitators for such opportunities. One interviewee requested specifically that engineers be allowed to meet and discuss overlaps.

Looking at earlier reported cases (Linåker et al., 2024), National Government OSPOs place particular emphasis on cultivating large, cross-government technical communities that support ongoing collaboration, knowledge exchange, and sustained engagement. The Italian OSPO's Developers Italia community exemplifies this, bringing together (at the time) more than 10,000 participants from diverse professional backgrounds to work on public-sector OSS projects and maintain shared resources. Similarly, the French OSPO coordinates the Blue Hats community, a growing collective of civil servants and external participants who use and develop OSS for the public sector. These communities serve not just as knowledge-sharing hubs but also as social anchors that normalise open collaboration and foster a shared identity around public-sector OSS practice.

In Kenya, a structured training programme is intended to create a core group of 100–150 OSS-capable staff across ministries, expected to become a community of practice that can help sustain OSS adoption. In Trinidad and Tobago, a similar community of practice is also being grown across ministries involved in pilot programs.

6.9.2 Multi-stakeholder advisory structures

Community-building may be complemented by formalised advisory bodies that institutionalise dialogue between public administrations and the wider OSS ecosystem. For example, France's free software council assembles representatives from both government and the broader community to deliberate on matters of strategic or operational concern. These structures function as boundary-spanning forums, enabling OSPOs to channel external expertise into internal decision-making while ensuring that public sector needs are heard within the wider ecosystem. A similar forum that brings together stakeholders and experts across the Danish OSS ecosystem would play a significant role in supporting the national OSPO structure, while also helping coordinate joint efforts and build common capabilities across layers of society.

6.9.3 Cross-government and cross-border collaboration

OSPOs frequently act as intermediaries and conveners, connecting PSOs with peers across municipalities, ministries, national agencies, and European partners where relevant. Local Government OSPOs, such as Bratislava's, maintain active communication channels with other cities, both domestically and internationally, and explicitly leverage the experience of more mature OSS cities like Amsterdam, Paris, and Barcelona. These collaborations are described as instrumental for acquiring best practices, growing confidence, and strengthening local capacities that would otherwise remain fragmented.

In Denmark, similar networking is facilitated, for example, between municipalities through OS2 for the development and initiation of common OSS projects. The regional digitisation associations, such as DIGIT[38] and GovTech Midtjylland[39] play a role in collaboration and in enabling the adoption of these solutions, including non-OS2 products.

[38] https://digitaliseringsforeningen.dk/
[39] https://govtechmidtjylland.dk/

From a cross-border perspective, a wider set of partners, including Local Governments Denmark (KL) and OS2, have collaborated with the Dutch Association of Municipalities (VNG) to evaluate the potential adoption of Signalen – an OSS application for reporting issues in public spaces. There are also reports of potential collaborations between OS2 products and its Swedish counterpart, Sambruk (Linåker et al., 2025a). At the supranational level, OS2 further engages in the European Commission's OSPO network through which European public-sector OSPOs exchange experiences, tools, and policy insights.

The European Digital Infrastructure Consortium for Digital Commons (EDIC-DC) is another example of countries such as France, Germany, the Netherlands, Italy, and Luxembourg collaborating on joint OSS-based commons. The collaboration is currently being established and centred around office productivity suites. Cross-border collaboration is also an important aspect in other geographical areas, as in East Africa, where Kenya is a driving force behind its joint roadmap for Digital Public Infrastructure (DPI). The National Government OSPO of Trinidad and Tobago describes a vision of a Caribbean-wide collaboration focused on OSS sharing and reuse.

6.9.4 Advocacy for cultural and organisational change

Advocacy is an equally central dimension, though typically embedded within broader operational work rather than carried out as a standalone activity. Several interviewees, including public-sector OSPOs, underline that building trust, reducing perceived risk, and challenging conservative procurement and sourcing cultures require sustained interpersonal engagement across organisational layers. General information campaigns and training is needed to raise knowledge and awareness.

The State OSPO of Schleswig-Holstein considers communication and advocacy among its main tasks for driving change. They focus on telling a consistent narrative internally to colleagues and leaders, and externally to municipalities, vendors, and European partners. The OSPO sees itself as leading change management, ensuring that everyone understands why OSS matters and how the State is moving in that direction. In this work, they help stakeholders understand OSS basics while reducing fear and risk aversion. A key message is that OSS is not only a technical choice but a sovereignty and resilience strategy. Still, they highlight that their approach is not punitive or centrally enforced, but rather relational, collaborative, and momentum-based. They explicitly avoid "building walls" and instead work to build trust and supportive relationships.

Trinidad and Tobago's National Government OSPO emphasises advocacy as one of its core activities and as a key to the change management process required. Roadshows, community centres, marketing, and public communication campaigns are all leveraged in the outreach.

In Association-based OSPOs, community management emerges as a core stewardship responsibility. Organisations like OS2 act as neutral custodians of shared OSS projects, mediating between member municipalities and suppliers, maintaining governance structures, and ensuring continuity. Their advocacy similarly takes the form of clarifying benefits, guiding municipalities through transitions, and providing structured pathways for collaboration, especially in contexts where resourcing and technical expertise differ widely across members.

6.10 Capability to provide training and build organisational competence

Summary:

Competence gaps remain one of the most persistent obstacles to OSS adoption and collaboration across the public sector. Many PSOs lack the skills needed for procurement, licensing, development practices, security, and community engagement. Public-sector OSPOs therefore play an important role in coordinating and delivering targeted training that supports both foundational literacy and specialised expertise.

Specifically, we find in the context of building OSS competence that public-sector OSPOs should consider:

- coordinating diverse training activities and delivery mechanisms, including workshops, seminars, community-driven sessions, national OSPO network events, internal programmes, and OSS ambassador schemes that help distribute knowledge across organisations.
- developing shared toolkits and reusable guidance, such as procurement guidelines, release processes, and documentation templates, enabling scalable and consistent training across PSOs.
- providing role-specific training, ensuring that policymakers, procurement officers, developers, legal teams, compliance staff, security specialists, service managers, and end-users each receive the knowledge needed to engage confidently with OSS.
- supporting both formal and informal learning, including peer review, mentoring, hackathons, and hands-on assistance that help embed open working methods in everyday practice.
- building competencies related to security and supply-chain sustainability, addressing misconceptions around OSS security and strengthening organisational readiness for long-term maintenance and compliance needs.

Below, we outline how OSPOs can organise and deliver these training activities and the themes most frequently highlighted as priorities for capability building.

6.10.1 Training activities and delivery mechanisms

Several means of disseminating knowledge and training have been reported and promoted. Workshops, seminars, and community-driven sessions have, for example, been shown to play an important role, especially given that OSPOs can be resource-limited. External communities such as Blue Hats in France and Developers Italia in

Italy support by organising workshops, technical sessions, and thematic seminars, helping civil servants build general OSS literacy, reduce uncertainty, and cultivate skills needed for collaboration. Wider or topic-focused conferences is requested by several interviewees as a means for engineers to meet and discuss ideas for common initiatives, and address common challenges.

The Dutch National Government OSPO highlights national OSPO networks as key for enabling PSOs to convene on common pain points, such as how to consider OSS in public procurement. The Swedish OSPO network provides another model, incorporating 60+ public and private organisations and their OSPOs, targeting similar topics to the Dutch, but also how European legislation, such as the Cyber Resilience Act (CRA), affects organisations and how it can be translated and considered from a national perspective.

Structured internal training programmes aimed at developers, legal teams, and middle management also play an important role. These programmes focus on helping staff understand the organisation's OSS strategy, navigate compliance, and adopt open working methods. Delivery is first-hand provided by any institution-centric OSPO. If not present, any overarching OSPO, such as a National Government or Association-based OSPO, would ideally support, though resources can be an issue. Creating an OSS ambassador program where local champions are trained to further disseminate training provides an extended resource to any OSPO.

Kenya and Trinidad & Tobago offer two highly complementary approaches to building national OSS competence: Kenya has developed a structured, year-long training pipeline that professionalises technical capacity through intensive five-day courses, certification-oriented modules, and parallel non-technical programmes for senior managers, all aimed at creating a sustainable community of practice within government. Trinidad & Tobago, meanwhile, pairs ministry-level technical upskilling with broad ecosystem development—training public servants, procurement regulators, private vendors, NGOs, and even planning for OSS literacy in schools—supported by nationwide awareness campaigns, roadshows, and hands-on pilot migrations that build confidence and reduce fear. Together, they illustrate a combined model where deep technical professionalisation (Kenya) is reinforced by whole-of-society cultural adoption and supplier-ecosystem growth (Trinidad), forming a holistic blueprint for scalable, long-term OSS competence.

By developing shared toolkits and repeatable guidance materials, training can be scaled and decentralised. Common procurement guidelines for considering OSS in an acquisition process, or guides on releasing software as OSS, are examples of valuable resources commonly shared and developed by OSPOs.

Formal training can also be complemented with informal mechanisms, including peer review, internal hackathons, hands-on support, and mentoring. These activities help embed collaborative habits into everyday work and allow teams to test and refine open-working methods in a low-barrier environment. These activities can be planned and executed at both the local and wider government levels, pending resource availability.

6.10.2 Role-specific training themes and target audiences

Training must help counter persistent misconceptions about OSS, build foundational literacy, and enable a shift toward open-by-default practices. This includes broad-based education for civil servants, IT departments, municipal staff, and political leadership. However, trainings must also be made direct and specific for different roles across public sector.

- Training for policy makers and executives must emphasise strategic use cases, required capabilities, and the organisational and cultural changes necessary for OSS to serve broader policy goals. Executive briefs and tailored communication formats help ensure that OSS is prioritised in line with national or institutional ambitions.
- Procurement officers require detailed, practice-oriented training to evaluate OSS options, understand inbound and outbound licensing considerations, and set correct requirements so newly developed software can be released as OSS. Such training positions procurement as an enabler rather than a barrier.
- Operational roles such as developers, legal specialists, compliance officers, and security teams need support in applying open working methods, assessing licensing obligations, and managing compliance processes, including the use of SBOMs.
- End-users, frontline staff, and service managers need special training to ensure sustainable adoption of municipal OSS solutions. Continuous user-oriented training is particularly critical for large, shared platforms such as e-service systems.
- A cross-cutting training theme concerns security and the sustainability of OSS supply chains. Training is required to address preconceptions around OSS security, clarify maintenance responsibilities, and build the competencies necessary for PSOs to contribute meaningfully to the sustainability of the OSS ecosystem they rely on.

7 Organisation of and roles within the support structure (RQ4)

Summary

A future support structure must reflect the realities of the Danish public sector. It needs to build on existing strengths, distribute responsibilities sensibly, and combine policy-shaping with practical enablement. The investigation highlights several considerations that should guide the design.

Specifically, we find that a Danish support structure should consider:

- Building on what exists. Denmark already has strong actors such as the Agency of Digital Government (Digitaliseringsstyrelsen), OS2, KOMBIT, DBC Digital and the Agency for Governmental IT Services (Statens IT). These should be connected and reinforced rather than replaced.
- Position the OSPO where mandate, authority, and feedback loops align. Institutional placement fundamentally shapes an OSPO's ability to translate policy into practice and coordinate coherent action across the public sector.
- Distributing capabilities across levels. A single OSPO cannot meet the diverse needs of municipalities, regions and agencies. A federated model with considering complementary OSPO archetypes (see Section 2.6) with national, regional and local roles avoids bottlenecks and ensures proximity to practice.
- Balancing and connecting policy work with technical enablement. Technological expertise is crucial for inputting and translating policy into practical guidance, and for aligning support and technology with policy and its explicit and implicit goals.
- Supporting inward- and outward-facing work. Where needs and resources preside, inward-facing OSPOs are needed, while outward-facing support is needed to scale. The latter can be provided with a national, regional, local, or cross-government scope.
- Embedding communication and change management. Cultural shifts require sustained narratives, trust-building and visible leadership.
- Ensuring sustainable stewardship. Long-term reuse depends on governance models that cover association-based, supplier-based, internal, and state-owned stewardship.

- Creating multi-level coordination mechanisms. A national OSPO network with federated OSPOs and support functions, with shared governance frameworks are essential for coherence.
- Treating funding as strategic. Stable funding is needed for both new OSS alternatives and maintenance of critical components.
- Prioritising reusable artefacts and automation. Templates, standards and automated compliance processes allow support to scale efficiently.
- Hiring staff to OSPOs and support functions that has proven OSS expertise, socio-technical understanding, and community trust.

Below, we expand on each consideration and its implications for a federated Danish

7.1 Key considerations for support structure

This section synthesises the empirical findings and related work into a concrete proposal for how Denmark can organise and scale support for OSS across its public sector. Our intent is to lay out technical, organisational, and policy-related design considerations that any support structure must account for if it is to deliver on broader goals such as digital sovereignty, interoperability, cost control, and innovation

7.1.1 Build on what exists

Denmark already has a fragmented but functionally rich ecosystem of actors performing OSPO-like responsibilities. A coherent support structure should amplify these roles and connect them rather than replacing them with a single central unit, such as a single National Government OSPO.

At the national level, the Agency of Digital Government (Digitaliseringsstyrelsen) provides policy instruments, architectural principles, procurement guidance (though limited), and interpretation of EU-level developments. This mirrors the role of typical National Government OSPOs, such as those in France and the Netherlands, which act as central translators of policy into practical guidance. These organisations illustrate that National Government OSPOs are not primarily engineering units (though ZenDIS in Germany is a notable exception), but rather interfaces between strategy and practice, articulating policy goals in ways institutions and municipalities can implement. The model is also reflected on the regional level of government in the state of Schleswig-Holstein.

At the municipal level, OS2 already functions as an association-based OSPO and steward responsible for governance frameworks, collaborative procurement, and stewardship of a substantial portfolio of shared OSS solutions. OS2 resembles the Dutch VNG and the Czech Open Cities (Linåker et al., 2024), which offer neutral governance structures, vendor engagement models, and collaboration mechanisms that municipalities can rely on when internal capacity is insufficient. Single municipalities such as Aarhus and Copenhagen further demonstrate resourcefulness and a driving force in the local and national change process.

Meanwhile, KOMBIT, DBC Digital, and the Agency for Governmental IT Services (Statens IT) have capabilities that align with institution-centric OSPOs such as the OSPO within the European Commission (Linåker et al., 2024) and with state-owned service-provider stewards (Linåker et al., 2025). These organisations already possess engineering capacity, internal development teams, and long-term operational responsibilities for critical digital services. Some similarities can also be drawn with the German Centre of Digital Sovereignty (ZednDIS), which operates both as an OSPO and as a steward of strategic products (OpenDesk) and platforms (OpenCode), illustrating a hybrid model that combines policy relevance with technical capability.

7.1.2 Position the OSPO where mandate, authority, and feedback loops align

Another central consideration concerns where in government an OSPO is situated, as its institutional placement fundamentally shapes its ability to translate policy into practice and to coordinate coherent action across the public sector. The interviews, particularly the UK case, highlight that the OSPO must be located at a central, authoritative point in government where strategic direction, operational expertise, and cross-government coordination naturally converge.

In the UK, early success in standardisation and platform consolidation stemmed from the fact that the responsible unit was embedded within the Cabinet Office, close to both the national CTO function and the machinery of cross-ministerial governance. This proximity enabled fast decision-making, strong legitimacy, and, crucially, tight feedback loops between policy, delivery, and standardisation efforts. The interviewee specifically stresses the importance of working and trust-based relationships between the OSPO, and the wider organisation (internal or external) it aims to support. The placement in the Cabinet Office was accordingly partial for the described success, but the relationships maintained across the ministries were as important. When the UK later separated policy from delivery into separate units, those relationships and feedback loops weakened, slowing alignment and increasing fragmentation, a lesson repeatedly emphasised as a cautionary tale.

The Kenyan National Government OSPO emphasises the importance of being hosted by the Ministry of Information and Communication Technology. The position signals a mandate which is crucial in proving legitimacy, gaining buy-in from other ministries, enabling collaboration, and organising training.

Placing an OSPO in a central, cross-government hubs with a clear mandate, hence, ensures it can translate high-level political ambitions into practical, actionable guidance, templates, and shared instruments that ministries, regions, and municipalities can adopt without ambiguity. The importance of mandate, trust-based relationships and positioning resonates across levels of government and institutions, and must be considered throughout the support structure if policy is to be translated into action.

7.1.3 Distribute capabilities

Another key consideration is that the Danish public sector is not homogeneous. Municipalities differ dramatically in size, digital maturity, and procurement capacity. Regions, agencies, and ministries face distinct operational and regulatory contexts. A single organisation cannot meet all these needs without becoming overwhelmed.

This insight is reflected broadly across European cases surveyed in this report. The German Centre of Digital Sovereignty (ZenDIS) explicitly notes that one-to-one consultancy cannot scale and has therefore shifted towards reusable templates, procurement guidance, and automated compliance tooling, something also confirmed in earlier studies (Linåker et al., 2024). The Dutch National Government OSPO, in turn, is designed not as a monolithic unit, but as an umbrella, coordinating OSPO efforts across ministries while leaving operational support tied to organisational contexts. The Schleswig-Holstein OSPO employs a dual model with formal strategy and communication at the centre, and a virtual OSPO supporting the wider parts of the region's PSOs, ensuring proximity to practice while maintaining strategic coherence.

For Denmark, responsibilities should be distributed across several OSPOs at various levels to allow support to be delivered at the right level of granularity, avoid dependency on a single team, and reduce the likelihood of bottlenecks. The different OSPO archetypes (see Section 2.6) across national, regional and local levels, including institution-centric, association-based, and academic OSPOs, should be considered as building blocks that can be combined and matched to best suit the needs from a national support structure at large.

7.1.4 Balance and connect policy-shaping with technology enablement

Policy ambitions alone do not lead to OSS adoption, reuse, or collaborative development; they must be operationalised through concrete tools, infrastructure, and governance mechanisms. A key consideration, therefore, is how OSPOs position themselves on the continuum between **policy-shaping** and **technology enablement**.

Cases surveyed show that meaningful impact arises where strategic direction is paired with practical enablers. The German Centre of Digital Sovereignty (ZenDIS) contributes to Germany's digital sovereignty strategy while simultaneously maintaining the two products OpenDesk and OpenCode, and providing hands-on procurement guidance.

The UK Government Digital Services (GDS) has a similar setup where policy shaping and translation are tightly connected with development, standardisation, and delivery of key technologies as the GOV.UK design system. An interviewee with long-term experience from the GDS emphasises the importance of this connection, as the technology enablement creates a feedback loop to policy and vice versa. Technological expertise and perspectives are critical to efficiently provide input to and transform policy into practical guidance, and understanding of policy with its explicit and implicit goals is crucial when implementing support and standardising infrastructure across government.

The National Government OSPOs in France and Italy while both small in size also connects both sides through its subset of highly skilled staff, managing to both balance and connect policy shaping with technology enablement by focusing on scalable support, such as catalogues, licensing templates, contribution guidelines, and community governance models that PSOs in the respective countries can adopt without reinventing processes (Linåker et al., 2024).

As put by one interviewee, OSPOs work best when embedded within a broader digital government capability, such as a central digital unit or digital service that sets service standards, architecture, and delivery practices, either internally for a specific organisation, or more broadly for a wider set of PSOs. Without that anchoring in institutional capability, OSPOs risk becoming compliance or advocacy units rather than strategic enablers.

In the Danish context, a National Government OSPO should ideally handle EU alignment, strategic guidance, and national templates, while remaining embedded in technology delivery and standardisation efforts. Potential Regional and Local Government OSPOs, and state-owned service providers should equally manage national alignment with regional and local policy, while providing the operational support necessary to implement these strategies. OS2, as an Association-based OSPO and Steward, in some senses already takes on a policy and technology-based portfolio, thereby contributing to and covering tasks of a potential National Government OSPO.

7.1.5 Enable both inward- and outward-facing support

OSPOs vary not only by level of government but also by orientation of their support. **Inward-facing** OSPOs support internal processes, such as intake mechanisms, licence compliance, developer enablement, and internal culture building. This is exemplified by the OSPOs of the European Commission and the Dutch Tax Administration, which focus on organisational maturity (Linåker et al., 2024).

Outward-facing OSPOs primarily support organisations beyond their own, and can have different **scope** with the support they provide, e.g., to PSOs on **national**, **regional** or **local levels of government**, or a **cross-government scope**, considering multiple levels together.

The Kenyan and Trinidad & Tobago National Government OSPOs focus explicitly on expanding cross-government training programs and communities, while also working with pilot ministries to transition from proprietary to OSS solutions, primarily with national government in scope. French, German, and Italian counterparts both maintain a more cross-government scope, developing shared tools, catalogues, procurement guidance, governance models, and communities of practice that can scale across PSOs on different levels of government.

Hybrid OSPOs combine both, as exemplified by the Dutch National Government OSPO, which aims to coordinate OSS policy across ministries while supporting shared ecosystem initiatives such as the Forgejo-based social code collaboration platform.

A Danish support structure should acknowledge and formalise these different orientations across a national support structure to ensure that policy alignment and practical guidance are disseminated and translated across levels of government and

PSOs. The setup will vary depending on an OSPO's position within the overarching structure and the support provided by other OSPOs or support functions.

7.1.6 Embed communication, storytelling, and change management

Several interviewees emphasised that OSS adoption is as much a cultural shift as a technical one. OSPOs, therefore, need strong communication functions that are capable of framing narratives, building coalitions, and maintaining alignment across diverse actors.

The Schleswig-Holstein OSPO demonstrates this clearly. Since its establishment, its most significant impact has come from articulating a coherent story about digital sovereignty and OSS, providing a consistent reference point for internal and external stakeholders, engaging municipalities, suppliers, and political leadership, and strategically communicating to manage expectations and maintain momentum.

Similarly, the Dutch OSPO stresses the importance of advisory work, advocacy, and visibility. The German Centre of Digital Sovereignty (ZenDIS) engages widely across ministries, vendors, and EU initiatives, reflecting the need for OSPOs to act as "boundary spanners" connecting policy makers with practitioners. The Trinidad & Tobago OSPO goes beyond ministries through roadshows and local engagement with community centres, teachers, and higher education institutions.

For Denmark, embedding communication, advocacy and change-management capacity within the national support structure and its OSPOs is essential for sustaining public sector confidence in OSS. OS2's model for vising and engaging with local governments can serve as inspiration.

7.1.7 Enable sustainable stewardship of public-sector OSS

A durable support structure must explicitly enable stewardship to ensure public-sector OSS remains available, trustworthy, and reusable. Stewardship is the governance layer that prevents person-dependence or vendor capture and underpins reuse, interoperability, and digital-sovereignty goals.

Denmark already has a strong association-based stewardship model through OS2 for widely used municipal solutions similar to Addulact in France and Open Cities in the Czech Republic. While mainly focused on the municipal level, OS2 provides potential a stewardship foundation for sustainable hosting and facilitation of projects also from other levels of government. Further PSOs, and the national support structure at large should consider the opportunities in building on what exists before creating new stewardships.

Still, depending on needs and possibilities, there are additional and complementary stewardship models to consider. These include the supplier-based stewardship for niche components with open-governance clauses to avoid de facto lock-in, government-internal stewardship for PSO-specific systems where strategic control and capability building are key, and state-owned service-provider stewardship for foundational infrastructure, but complemented by open governance to avoid closed

operational habits. In France and Germany, the National Government OSPOs also have a form of stewardship-based role.

Denmark should consider the needs of all parts of the public sector, expand stewardship capabilities as needs emerge, taking a point from OS2, and as needed, consider the different stewardship archetypes available.

7.1.8 Create multi-level coordination mechanism

A federated support structure requires deliberate coordination mechanisms. Without them, policy ambition will fail to translate into coherent practice across government levels.

The surveyed cases underline the importance of such mechanisms. The Dutch National Government OSPO operates within a newly established CIO ecosystem that connects ministries around shared priorities. The German Centre of Digital Sovereignty (ZenDIS) collaborates across federal, regional, and municipal layers and participates in transnational efforts such as EDIC-DC. Schleswig-Holstein's regional OSPO convenes a state-level task force that involves key service providers, political leadership, and technical teams.

Existing coordination mechanisms should be specifically evaluated and considered for reuse. OS2, e.g., already organises a large part of the municipalities in Denmark and has governance and coordination mechanisms set up in relation to its association-based collaboration structure, spanning multiple projects under active development. The Agency of Digital Government, together with KL, organises a broader, coherent collaboration through the working groups related to the national architectural principles.

For Denmark, key coordination mechanisms could include:

- a national OSPO network anchored in a National Government OSPO (such as the Agency for Digital Government, OS2 or a comparable institution),
- Regional Government OSPO(s) providing proximity support and aggregation for the Danish Regions,
- Local Government OSPO(s) providing proximity support and aggregation for the Danish municipalities,
- shared governance models for catalogues, social code collaboration platform, and procurement frameworks,
- structured feedback loops between local, regional, and national levels, and
- clear escalation and decision-making pathways

7.1.9 Treat funding as a strategic design parameter

Funding profoundly shapes the sustainability and reach of OSS support structures and is critical for addressing gaps in the digital infrastructure.

The German Centre of Digital Sovereignty (ZenDIS) benefits from a subscription model via OpenDesk, providing a stable revenue stream to supplement federal funding while also investing in the product's development. The Dutch equivalent solution, the MinBjeru initiative, illustrates how fragile progress becomes when project funding is

fragmented or short-term, especially when national and municipal priorities diverge. The case of Schleswig-Holstein's micro-funding scheme further demonstrates how small, targeted amounts can stimulate adoption, build trust, and signal political commitment.

In Denmark, the gap has been highlighted across interviews, where the need for funding streams is critical for successful and sustainable OSS adoption. Funding, accordingly, needs to cover both:

- strategic investments for developing new alternatives, running feasibility studies, and seeding collaborative projects; and
- maintenance and security for critical OSS infrastructure and long-term stewardship, similar to the approach taken by Germany's Sovereign Tech Agency.

Without stable funding, no support structure, regardless of its design, will achieve sustained impact, with dependencies reinforcing themselves on the cost of strategic autonomy.

7.1.10 Reduce bureaucracy through reusable artefacts and automation

Finally, the support structure needs to scale its support and resources as far as possible by providing reusable artefacts rather than focusing too much on individual consultancy or bespoke casework, which comes at a cost.

National Government OSPOs use catalogues, procurement templates, and compliance automation to reduce administrative burden. Association-based OSPOs, such as the Danish OS2 and Dutch VNG, provide governance frameworks that local PSOs can adopt without having to design them from scratch.

For Denmark, prioritising reusable artefacts and automation will enable scaling support across PSOs with widely varying capacities and resources.

7.1.11 Ensuring the right expertise and community trust in OSPO staffing

Establishing an effective OSPO requires not only formal structures and processes but also the right people. OSS work is inherently socio-technical, and its success depends on individuals who understand both the technical dynamics of OSS development and the social fabric that sustains it. Public-sector OSPOs and related support functions therefore need staff with deep OSS expertise, people who are familiar with contribution workflows, licensing nuances, stewardship practices, and community governance models. Equally important is community trust: OSPO personnel must be individuals who can credibly represent public-sector interests in open-source communities, engage constructively with maintainers and contributors, and build bridges rather than friction.

Hiring should deliberately seek candidates with demonstrated OSS contributions, community participation, experience stewarding projects, and the interpersonal skills

necessary for collaboration across diverse ecosystems. Such expertise enables OSPOs to assess the health of upstream projects, guide PSOs in selecting sustainable solutions, and participate meaningfully in European and global OSS initiatives. It also ensures that the public sector speaks with legitimacy when shaping standards, governance frameworks, and interoperability efforts.

7.2 Architectural options for a multilevel support structure

Summary:

This section compares three organisational models for how OSS support can be structured. The aim is to clarify their trade-offs and identify the model that best fits Denmark's governance structure, existing actors, and capability needs.

Centralised model
A strong national OSPO offers clarity, uniform guidance, and a single point of accountability. It simplifies political signalling, supports consistent policy translation, and enables rapid dissemination of standards. However, it does not match Denmark's decentralised administration. A single unit would struggle to meet diverse municipal needs, risk becoming a bottleneck, and underutilise existing actors. Fully centralised approaches elsewhere also rely on surrounding ecosystems to scale.

Decentralised model
A decentralised model gives PSOs autonomy to adapt OSS practices to local needs and supports rapid experimentation. Yet without shared catalogues, templates, or coordination mechanisms, fragmentation grows. Smaller PSOs lose out, duplication increases, and national goals for interoperability and sovereignty become difficult to realise. Experiences from Sweden show that decentralisation alone stalls scaling and reuse.

Federated model
The federated model distributes responsibilities across national, regional and local OSPOs, supported by shared infrastructures, templates, governance mechanisms and coordinated workstreams. Policy is shaped centrally while implementation is enabled locally. International examples show elements of this approach emerging, though rarely fully realised. For Denmark, the federated model aligns strongly with existing capabilities, respects municipal autonomy, addresses diversity of needs, and enables scalable support. It requires deliberate coordination, clear mandates, and shared artefacts, but offers the most resilient and future-fit structure.

Below, we expand on the federated model and outline how it can be designed for Denmark.

7.2.1 Centralised model

The centralised model focuses on a single, strong national unit (a National Government OSPO) where the majority of core functions are concentrated, including policy translation, procurement enablement, compliance and licensing guidance, shared

collaboration infrastructure, measurement and follow-up, and, in some variants, also elements of stewardship.

The model creates a central point of accountability, which simplifies political signalling, policy translation (e.g., CRA/IEA), and publication of uniform templates and metrics. Common policies and practices can potentially be standardised and disseminated quickly and consistently. The model also provides a single national entry point, simplifying engagement with the market.

On the other hand, a central unit would struggle to meet highly varied municipal and agency needs (e.g., procurement coaching, release support, local onboarding). Over time, this could produce bottlenecks and erode trust. A centralised approach further risks sidelining existing actors that already perform OSPO-like roles. Denmark's decentralised administration and strong municipal autonomy also make it hard to adopt one-size-fits-all instruments without local adaptation.

For example, the National Government OSPOs in France and the Netherlands help set direction and define instruments, but they do not bear the full operational burden alone. Germany's Centre of Digital Sovereignty (ZenDIS), an outlier with both a policy-guiding and technical-enabling role, still depends on surrounding regional actors and service providers; even there, case-by-case consultancy does not scale and is supplemented by reusable artefacts and automation.

For Denmark, a fully centralised model would not, accordingly, fit. It offers clarity but would likely create a gatekeeping node, underuse existing actors, difficulties in scaling support, and fail to respond to diverse local contexts.

7.2.2 Decentralised model

In a decentralised model, each ministry, PSO, region, or municipality independently defines OSS policies, processes, infrastructures, and collaboration arrangements. Coordination is voluntary, and shared assets emerge sporadically. This enables organisations to tailor approaches to local constraints, legacy systems, and risk profiles. Pilots can move quickly and generate context-specific learning.

In the background, without common catalogues, platforms, or templates, PSOs will repeatedly solve the same problems, increase transaction costs, and limit reuse. Adoption becomes uneven and fragile as smaller PSOs lack access to practical support. National goals, e.g., in terms of digital sovereignty and interoperability, will be hard to reach when practices diverge and measurement is weak.

Considering earlier reports, decentralised modes have typically dominated in early stages of the evolutionary process for OSS support structures, with countries moving to strengthen more centralised modes of governance and resources, such as national collaboration infrastructure, association-based stewardships, and coordination mechanisms, aimed at countering fragmentation.

Sweden is one example that currently maintains a very decentralised support structure, with loose coordination mechanisms, and strong single actors that drive the development of practice and infrastructure, as well as policy development. Still, scaling and adoption are general challenges with collaboration and reuse, which are highly

fragmented. A recent report from the Swedish Agency for Digital Government signals a move towards a more centralised model, yet uncertainty over funding and implementation remains a risk (DIGG – Myndigheten för digital förvaltning, 2025).

For Denmark, a purely decentralised model would entrench current fragmentation and slow progress on reuse and sovereignty. It may be suitable for early discovery in niche domains, but not as a national default.

7.2.3 Federated model

In the Federated model, responsibilities are distributed across levels of government and OSPO archetypes. The various OSPOs are coordinated through shared infrastructures, common templates, and structured governance. Policy is shaped centrally, and implementation is enabled locally.

Among the surveyed cases, the federated model is not commonly present; rather, it is a vision and a pathway for many countries. Germany, on the one hand, signals a centralised approach through the intent and scope of its Centre of Digital Sovereignty, which shows both promise and limitations in scaling support. On the other hand, the state of Schleswig-Holstein shows how decentralised efforts at the regional level can help address issues at scale, not just in support but also in communication, advocacy, and cultural change management. As the remaining states show far less interest in OSS, there is still a long way to go towards a federated model, yet signs are promising.

Looking at the Netherlands and France, both countries have a National Government OSPO, though DINUM in the latter case is more mature and comprehensive, with a similar scope and structure to ZenDIS in Germany. A clear difference is that DINUM has an interministerial function, with established, mandated coordination and support across ministries at the national level. The Netherlands is seeking a similar interministerial function through its national CIO network. Both France and the Netherlands also have strong or emerging Association-based stewards in the cases of Addulact and VNG, respectively. Both countries also have resourceful municipalities with significant investment and influence, namely Paris and Amsterdam.

Both countries, however, lack a regional mid-layer within their national support structures, as demonstrated by the State of Schleswig-Holstein. Italy has earlier signalled its intent to establish Regional Government OSPOs, e.g., in the Lombardy Region, yet the status remains unknown. In other countries, such as Spain, regions like Galicia and Andalusia demonstrate mature Regional Government OSPOs, while a clear National Government OSPO is absent (Linåker & Muto, 2024).

For Denmark, the federated model is the most fitting per this report, and should be designed from the start. The model leverages existing actors, provides scalable and proximity support, balances policy and practice, and enables resilient governance. The latter also poses risks, with many actors involved and across different scopes and cultures. Strong coordination mechanisms are therefore required, e.g., through a national OSPO network with clear mandates, time-boxed workstreams, and shared artefacts to keep alignment costs low.

7.3 Proposed Danish OSPO-based support structure

Summary:

Building on the considerations outlined in Section 7.1 and the comparative architectural analysis in Section 7.2, this section presents a pragmatic and federated support structure for Denmark. The model reflects the Danish governance context - decentralised, multi-actor, and capability-uneven - while drawing on empirical lessons from European reference cases. It is designed to grow and coordinate the capabilities necessary for public-sector OSS adoption, reuse, collaboration, and stewardship, as detailed in Section 6, and to connect these capabilities across levels of government through a coherent national OSPO network.

The structure comprises four main elements:

- A National Government OSPO anchoring policy translation, national instruments, shared infrastructures, and cross-government coordination.
- Regional Government OSPOs and Association-based OSPO(s) providing proximity support, localisation of guidance, and aggregation of regional and municipal needs respectively.
- Local Government OSPOs and Institution-centric OSPOs embedded where need and capacity align in local governments and single organssations (regardless level of government), and are focused on internal governance, intake/release processes, and developer enablement.
- Supporting national functions, including stewards, a project brokerage, procurement bodies, and funding programmes, that ensure the long-term sustainability, discoverability, and operationalisation of shared OSS projects.

Together, these entities form a distributed yet coordinated ecosystem capable of delivering the technical, organisational, and policy-related support that Denmark requires to scale OSS-based collaboration and improve digital sovereignty.

The subsections below define each component.

OSPO-types described below builds and extends general practice and OSPO archetypes observed and generalised across the European public sector (Linåker et al., 2024), as further described in section 2.6.

7.3.1 National Government OSPO – aggregated support on the national level and cross-government coordination

The National Government OSPO[40] serves as the central coordinating and strategic node for Denmark's public-sector OSS efforts. It provides the link between national policy and operational practice by translating EU and national ambitions into actionable guidance, templates, and infrastructures. It leads the development and implementation of national OSS strategies; coordinates cross-government communities; oversees national metrics and follow-up; and anchors training and capability-building initiatives. The OSPO also serves as Denmark's interface with national and international policymakers, European OSPO networks, and adjacent initiatives related to interoperability, data governance, and digital sovereignty.

Its orientation is **primarily outward-facing**, and, in the long term, primarily providing direct support for PSOs on the national level of government. In the short term, hands-on support is also provided to regional and local levels of government as regional and local government OSPO(s) are formed and matured.

The National Government OSPO may also serve the host organisation internally. Its placement is critical, ideally within a central and authoritative body that can provide the mandate needed to translate policy into support and technological enablement. The connection and feedback loops between policy and technology is also crucial to consider in the placement of the OSPO.

The Agency of Digital Government (Digitaliseringsstyrelsen) provides a suitable host, as it already operates a wide mandate and standard setting function interfacing with EU policy, maintaining and coordinating national architectural frameworks, while also developing and hosting key digital infrastructure projects. Policy translation and technology delivery accordingly align, providing the necessary feedback loops and outreach across the national, regional, and local levels of government.

Core functions include:

- Translate EU and national policy into guidance, processes, templates, and instruments.
- Oversee and ensure development and provisioning of procurement support, including model clauses, scoring criteria, and supplier-evaluation frameworks.
- Govern the national OSS catalogue and social code collaboration platform.
- Promote secure and compliant development and release of OSS.
- Convene and support national communities of practice and training initiatives.
- Maintain national metrics and follow-up on progress toward strategic goals.
- Coordinate and support the broader national OSPO network.
- Support funding streams in prioritisation and investments into innovation and maintenance within strategi areas.

[40] See section 2.6.1.

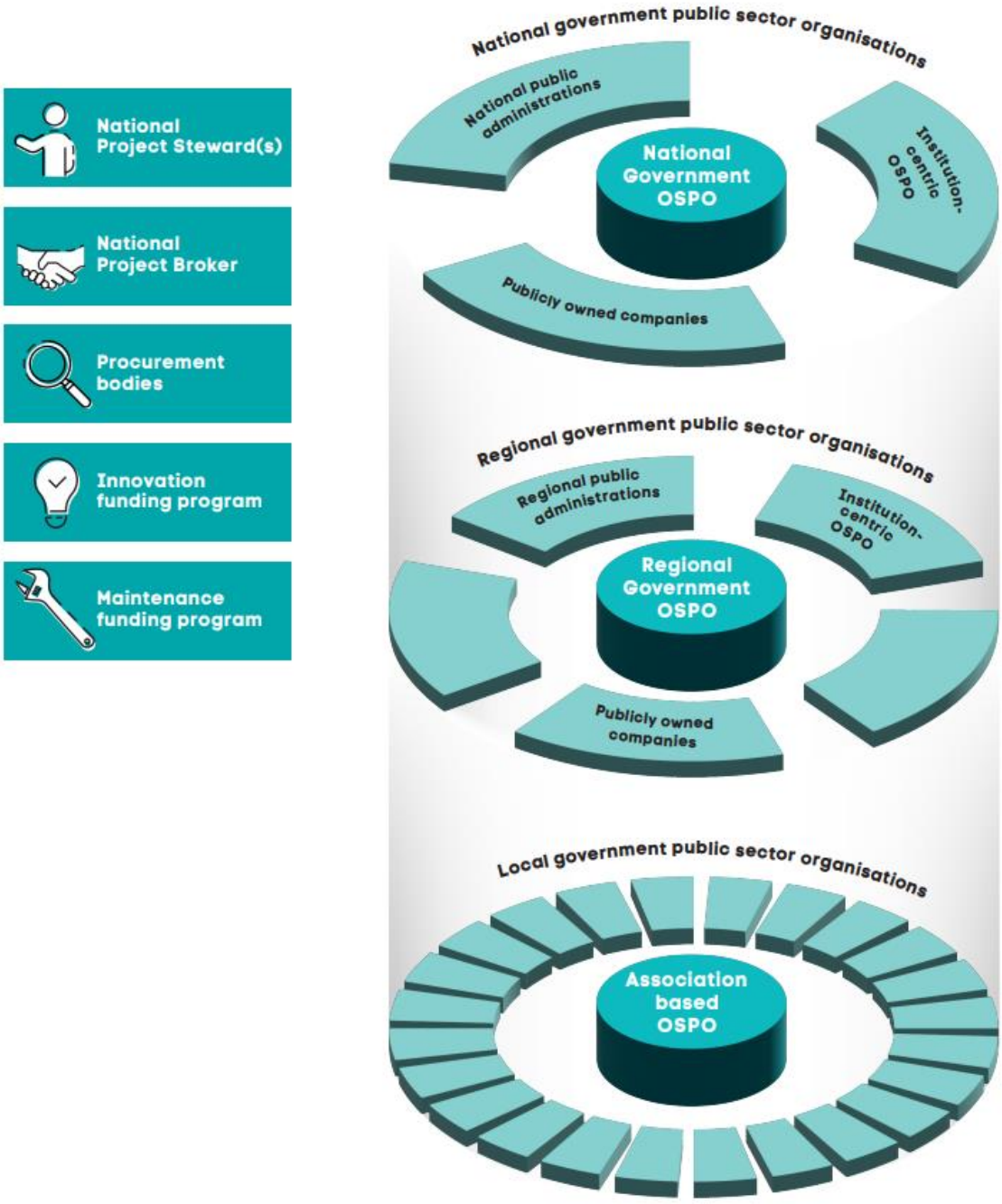

Figure 3: Overview of the national support structure, including the National Government, Regional Government and Association-based OSPOs supporting the national, regional and local levels of government respectively. Institution-centric OSPOs may be present across all levels. Local government OSPOs occur within single resourceful municipalities. National support functions as the National Project Steward and Project Broker supports the whole network.

7.3.2 Regional Government OSPO – aggregated support and coordination on the regional level

For the five Danish Regions, a joint Regional Government OSPO is proposed to provide coordinated and proximity-based support, hosted at one of the Regions, or through a common-owned entity. The OSPO integrates and extends support from other parts of the support structure, but focus specifically on the needs and use cases of the Danish Regions. Design aspects such as mandate and authority, as well as the link between policy translation and technological enablement, are again important to consider.

Core functions include:

- Provide hands-on support in procurement, licensing, and intake/release processes.
- Localise national guidance to regional contexts.
- Support joint regional initiatives and pilots aligned with national priorities.
- Facilitate regional communities of practice and training activities.
- Aggregate bottom-up needs and escalate them to the National Government OSPO.
- Report regional metrics and contribute to national follow-up.

7.3.3 Association-based OSPO – aggregated support and coordination on the local government level

For the Danish municipalities, the Association-based OSPO model[41] is proposed to be implemented either on a national level through OS2, or on a regional level through the planned regional IT-operation centres, each to be co-owned by the respective region's municipalities. As OS2 is already established, has experience and practice, and maintains an ecosystem of municipalities and suppliers, they should be considered as a primary candidate, with the regional IT-operation centres as providers of infrastructural support. Design aspects such as mandate and authority, as well as the link between policy translation and technological enablement, are again important to consider.

Core functions include:

- Provide hands-on support in procurement, licensing, and intake/release processes.
- Localise national guidance to local government contexts.
- Support joint local government initiatives and pilots aligned with national priorities.
- Facilitate local government communities of practice and training activities.
- Aggregate bottom-up needs and escalate them to the National Government OSPO.
- Report local government metrics and contribute to national follow-up.

[41] See section 2.6.3.

7.3.4 Local Government OSPOs – local and focused support and community enabler

Local Government OSPOs[42] are embedded in resourceful municipalities where there are sufficient organisational capacity and political mandate. Their focus is typically inward-facing, embedding policies, supporting developers and procurement officers, ensuring compliant intake and release processes, and participating in shared projects. At the same time, they play an important enabling role in wider collaborations and strategic projects, e.g., as Aarhus in the contexts of OS2 and OS2ai. Design aspects such as mandate and authority, as well as the link between policy translation and technological enablement, are also important to consider also on this local level.

Core functions:

- Implement internal policies, decision processes, and compliance routines.
- Support developers, procurement officers, and internal teams in working openly or through Inner Source.
- Participate in national, regional, and local level communities of practice.
- Contribute organisational insights to shared governance processes.
- Act as internal advocates and capability-builders.

7.3.5 Institution-centric OSPOs – internally focused support for resourceful organisations

Institution-centric OSPOs[43] are embedded in resourceful PSOs (despite level of government) where needs, priorities, and resources align. As with Local Government OSPOs, their focus is typically inward-facing, embedding policies, supporting developers, ensuring compliant intake and release processes, and participating in shared projects.

These OSPOs provide day-to-day guidance that cannot be centralised and ensuring that national frameworks translate into organisational practice. Design aspects such as mandate and authority, as well as the link between policy translation and technological enablement, are also important to consider.

Dedicated OSPOs may be specifically warranted in domains with special requirements, such as the medical domain where software must be quality and risk controlled. In these cases, the OSPOs has to work under a certified quality management system (ISO 13485), as exemplified by one interviewee. Other domains may face similar special requirements.

Potential cases for Institution-centric OSPOs includes KOMBIT, Agency for Governmental IT Services (Statens IT), Danish Court Administration (Domstolsstyrelsen), Danish Road Traffic Authority (Færdselsstyrelsen), and Agency of Digital Government (Digitaliseringsstyrelsen).

[42] See section 2.6.2.
[43] See section 2.6.4.

Core functions:

- Implement internal policies, decision processes, and compliance routines.
- Support developers and internal teams in working openly or through Inner Source.
- Participate in communities of practice.
- Contribute organisational insights to shared governance processes.
- Act as internal advocates and capability-builders.

7.3.6 Supporting national functions

A federated structure requires coordinated supporting functions that cut across all OSPO levels. These functions address stewardship, discoverability, procurement, and funding, which are core requirements for enabling OSS collaboration and reuse at scale.

7.3.6.1 National Project Stewards

National Project Stewards host and facilitate governance for public-sector OSS projects. They provide frameworks for initiating and maturing projects, establishing community processes, coordinating vendor ecosystems, and supporting pooled procurement. Stewards collaborate closely with the national OSPO network to ensure alignment with national guidelines and shared standards.

OS2 already represents a mature steward body, though mainly limited to municipal use cases. Expanded scope and responsibilities for OS2 to also consider OSS projects from and across regional and national levels of government should be considered first hand. If needs and requirements does not align, additional stewardship models should be investigated and implemented.

7.3.6.2 National Project Broker

The National Project Broker ensures that PSOs can find, reuse, and collaborate on OSS solutions. It maintains a national solution catalogue aligned with public-code.yml and operates a national, government-grade social code collaboration platform that enables open and Inner Source development. It also hosts templates, CI pipelines, SBOM tooling, and quality checks.

The broker can, e.g., be co-located with either the National Government OSPO or a steward organisation as OS2.

7.3.6.3 Procurement bodies

Procurement bodies such as SKI and the Advisory Unit for Procurement Program under the Agency for Public Finance and Management (Rådgivningsenheden Statens Indkøb - Økonomistyrelsen) support PSOs in procurement across the board and maintain framework agreements that can be leveraged in OSS-based acquisitions. Their role is proposed to be expanded to include providing OSS and sovereignty-aware requirements, templates, evaluation models, and supplier-qualification criteria, developed in collaboration with the National Government OSPO and the broader OSPO network.

7.3.6.4 Funding bodies

Dedicated and sustained funding is essential to support sustainable, realistic alternatives in strategic areas and to advance overarching policy goals such as digital sovereignty. Two programmes are needed specifically:

- Innovation and seed funding for strategic, high-impact OSS alternatives and feasibility studies. The programme should take explicit inspiration from the German Prototype Fund and the micro-investments programme in Schleswig-Holstein.
- Maintenance and security funding for critical OSS components and supply-chain improvements. The programme should take explicit inspiration from the Sovereign Tech Agency in Germany.

These funding bodies should collaborate closely with the National Government OSPO and stewards to define priorities, review applications, and monitor impact. They may be co-located with the National Government OSPO or an existing national funding entity, e.g., within research and innovation. A tripartite annual fund via the Danish government, Local Governments Denmark (KL), and the Danish Regions has demonstrated value in isolated rounds, and could prove a potential model for taking joint responsibility for the national digital infrastructure.

7.3.7 National OSPO Network

All OSPO entities, together with stewards, project broker(s), procurement bodies, and funding bodies, form the National OSPO Network. The network is the operational backbone of the model, ensuring shared ownership of national guidance, bidirectional information flow, and consistency in how OSS practices are interpreted and applied.

The network is convened and coordinated by the National Government OSPO, but is deliberately designed to avoid centralised gatekeeping. Work is organised through thematic workstreams such as procurement, compliance and licensing, governance of collaboration infrastructure, cyber security practice, training and capability-building, metrics and follow-up, and cross-border alignment, each co-led by the National Government OSPO and representatives from relevant parts of the national OSPO network. This ensures that regional and local perspectives systematically shape national instruments and that guidance evolves responsively.

For large-scale shifts (e.g., sovereign desktop options and office productivity suites), the national OSPO network can serve as an enabler for coordination and phased rollouts.

7.4 Maturity model and evolution path

Summary

The development of a national, federated support structure for OSS requires a sequenced, capability-building approach. The maturity model defines how Denmark can move from today's fragmented practices to a coherent, resilient ecosystem that supports national digital sovereignty.

Stage 0 – Foundational Planning and Alignment
Establishes the mandate and minimal structures needed to begin coordinated action. A National Government OSPO is set up within the Agency for Digital Government and staffed with OSS expertise and community trust as key requirements, an OSPO Network is formed across key actors, initial strategy work begins, and prototypes for essential guidelines and processes, as well as the national OSS catalogue and social code collaboration platform are launched.

Stage 1 – Structural formation and early community
Builds up focuses on validating early tools, processes, and support functions. A Regional Government OSPO is established, and OS2 is formalised as an Association-based OSPO responsible for scaling OSS support across municipalities. Procurement templates with sovereignty requirements are drafted and evaluated, intake and release processes are formalised, communities of practice emerge, stewardship pathways for OSS project archetypes are defined, and initial training builds basic competence across PSOs.

Stage 2 – Federated foundations and structured support
Matures support through revised processes and guidelines based on lessons learned, national funding programmes are launched, and communities of practice mature into national working groups supported by shared governance and maintenance cycles.

Stage 3 – Coordinated scaling and institutionalised practice
Formally embeds OSS considerations into procurement, compliance, and development routines. Reuse becomes standard practice, compliance processes and SBOM based checks are widely adopted, and multi year funding strengthens critical shared infrastructure.

Stage 4 – Embedded, resilient, and strategically aligned ecosystem
Completes the transition. Open by default becomes routine where appropriate, long term stewardship and funding are stable, and Denmark actively contributes to European digital commons while maintaining a metrics driven, sovereignty aligned digital ecosystem.

Figure 4: Five stage maturity model prescribing how the national support structure can evolve and mature in a coherent and systematic approach.

Several maturity models have been proposed for OSS adoption and for guiding OSPOs in growing an organisation's organisational readiness (TODO Group, 2025). These typically start from a present stage where OSS is used but unmonitored, and without any monitoring, coordination, strategic intent, or governance. As awareness grows, training, governance, and processes are set up to enable use, development, and collaboration, aligning with legal and security risks as they are being acknowledged by senior management.

In the next stage, contributions and engagement are typically structured and actively promoted through intensified training and advocacy, as well as refined processes, governance, and infrastructure for collaborative inner and open source development, yet still without a general strategy. With time, strategic intent grows through investments in creating new communities and through priorities that guide contributions and collaborations to align with business or policy goals. Finally, OSS is considered a strategic tool and is leveraged across the organisation to influence and steer broader ecosystems, industries, or parts of society in alignment with organisational goals.

The proposed model takes a similar phase-based approach, acknowledging that OSS use and adoption are currently fragmented and low, while several forerunners are present and more mature than others. Each phase represents an increased level of maturity for the national support structure as a whole and should be evaluated accordingly.

For each of the five stages, recommendations are mapped against capabilities presented in section 6. For simplification, capabilities are abbreviated as follows: Policy Strategy (6.1), Policy Instruments (6.2), Prioritisation & Migration (6.3), Infrastructure (6.4), Compliance (6.5), Stewardship (6.6), Measurement (6.7), Inner Source (6.8), Advocacy (6.9), and Training (6.10). Note that the list of recommendations is not a complete list of actions or recommendations. Readers are advised to consult section 6 for further details and activities that public-sector OSPOs and a national support structure should consider.

7.4.1 Stage 0 – Foundational planning and strategic alignment

The purpose of this stage is to establish the mandate, legitimacy, and minimal viable structures required to coordinate national OSS efforts. It lays the institutional and strategic foundation upon which all subsequent stages depend.

- Policy Strategy
  - Establish the National Government OSPO with an explicit mandate from national government, dedicated base funding, and 2–3 initial FTEs with proven OSS expertise and community trust.
  - Form the National OSPO Network by connecting existing actors with roles in OSS, procurement, digital architecture, and digital sovereignty, including the Agency of Digital Government (Digitaliseringsstyrelsen), Local Governments Denmark (KL), OS2, KOMBIT, Statens IT, DBC Digital, Danish Court Administration[44] (Domstolsstyrelsen), Danish Road Traffic Authority (Færdselsstyrelsen), SKI, along with active regions and municipalities.
  - Define scope, governance, resources, and hosting arrangements for Regional Government and Association-based OSPOs, supported by explicit mandates from national, regional, and local governments.
  - Draft the initial national strategy and roadmap for how OSS shall be used to grow and promote digital sovereignty, including broad consultation across national, regional, and municipal PSOs.
- Policy Instruments
  - Begin preparing process descriptions and guidelines for inbound and outbound OSS.
- Prioritisation & Migration
  - Conduct an initial scoping of key software, infrastructure, and vendor dependencies across PSOs to identify where deeper dependency mapping and risk analysis will be required in subsequent stages.
- Stewardship
  - Appoint OS2 as a National Project Steward and as the primary governance host for new public-sector OSS projects, with an aim for growing cross-government adoption and community.
- Infrastructure
  - Appoint role of National Project broker, and develop and operate prototypes of a national OSS catalogue and social code collaboration platform, including an open testing programme for PSOs and suppliers.

[44] https://www.domstol.dk

7.4.2 Stage 1 – Structural formation and early community build-up

The purpose of this stage is to validate early support functions, test concrete tools and processes, and build confidence across PSOs through hands-on pilots and initial communities of practice.

- Policy Strategy
  - Establish a Regional Government OSPO with clear mandates and 2–3 initial FTEs with proven OSS expertise and community trust delivering proximity support to the Danish Regions and related PSOs.
  - Formalise role of OS2 as an Association-based OSPO with responsibility for supporting municipalities, with sufficient additional funding and staffing to ensure ability to scale support to all Danish municipalities.
  - Initiate participation in cross-border OSS and digital commons efforts, including full and formal membership in EDIC-DC, and actively adopting and contributing reusable components to align Denmark with European digital infrastructure development.
- Policy Instruments
  - Draft procurement templates with sovereignty requirements (e.g., based on the EU Cloud Sovereignty Framework, with specific considerations related to OSS and open standards) and evaluate feasibility considering buyer and supplier sides.
  - Formalise intake and release processes and guidelines with decision support, templates, and risk classifications applicable across PSOs.
- Prioritisation & Migration
  - Pilot detailed dependency mapping and risk analysis in a sample of PSOs across levels of government to test methods and generate early insights for prioritisation.
  - Develop and test prioritisation criteria for replacing dependencies based on sovereignty impact, risk severity, technical feasibility, cost, and lifecycle timing.
- Infrastructure, Compliance, Inner source
  - Initiate formal operation of the OSS catalogue and social code collaboration platform with mandatory metadata (public-code.yml), automated compliance checks, and guided onboarding workflows.
- Compliance
  - Provide curated licence lists, OSS compatibility guidance, and basic compliance checklists to support procurement pilots and early intake processes.
- Stewardship
  - Outline, evaluate, and formalise stewardship and governance models needed for different OSS project archetypes, e.g., considering use case and level of government.
  - Based on evaluation, plan for and implement any additional National Project Stewards if needed.
- Training, advocacy

    - Deliver initial role-specific training for procurement officers, architects, developers, managers, and form communities of practice around procurement, development, architecture, and reuse.
- Advocacy, Inner Source
    - Develop a national communication and advocacy plan to build awareness of dependency risks, sovereignty goals, and OSS migration opportunities among PSOs and political leadership.
    - Enable Inner Source by promoting PSOs to share code, documentation, and early prototypes government-internally on the national collaboration platform, providing a low-risk way to practice open development before public release.

7.4.3 Stage 2 – Federated foundations and structured support

The purpose of this stage is to establish coordinated, scalable support structures across levels of government, anchored in shared platforms, governance models, and funding mechanisms.

- Policy Instruments
    - Translate dependency and risk findings into updated procurement templates, process descriptions, guidelines, ownership decision rules, and consideration of sovereignty requirements to guide PSOs in acquiring or developing replacement solutions.
- Prioritisation & Migration
    - Conduct a coordinated national dependency mapping across PSOs, produce a national risk map identifying high-impact proprietary dependencies, and develop a prioritised multi-year roadmap for OSS migration in strategic domains.
    - Apply prioritisation criteria nationally to produce a sequenced roadmap distinguishing short-term substitutions, medium-term migrations, and long-term investments.
    - Define and align a standard and reference implementation roadmap for underpinning digital infrastructure, taking point from the Deutschland-stack.
    - Launch national innovation funding and maintenance funding programmes to support development of strategic OSS alternatives and sustain critical shared dependencies.
- Infrastructure
    - Integrate dependency and risk metadata into the national OSS catalogue and collaboration platform, including optional tagging of high-risk components, recommended alternatives, and maturity indicators.
- Stewardship
    - Based on defined OSS project archetypes and any additional stewards, define processes and structures for governance, community management, development, and maintenance arrangements, including involvement of service suppliers, taking point from OS2 practice.
- Measurement

    - Develop and operate a national OSS measurement framework and dashboard, including indicators for dependency reduction, reuse levels, compliance activity, supplier ecosystem growth, and stewardship performance.
- Advocacy, Training, Inner Source
    - Scale communities of practice into national thematic working groups, enabling coordinated problem-solving and alignment on architectures, standards, and development methods.
    - Support Regional Government and Association-based OSPOs in running local engagement activities, roadshows, and briefings to broaden uptake.
    - Promote Inner Source for building and reusing shared components across PSOs, reducing duplication and supporting early development of OSS alternatives identified through dependency mapping.

7.4.3.1 Stage 3 – Coordinated scaling and institutionalised practice

The purpose of this stage is to embed OSS considerations across procurement, compliance, and development processes, enabling consistent reuse, shared components, and coordinated roll-outs across Danish PSOs.

- Policy Instruments
    - Integrate OSS requirements, scoring criteria, ownership rules, and exit clauses into national procurement frameworks via SKI and Statens Indkøbsprogram, and require justification when catalogue alternatives are not reused.
    - Require procurement processes to document how identified high-risk dependencies were addressed, mitigated, or replaced during acquisition.
- Prioritisation & Migration
    - Provide multi-year funding for strategic OSS solutions and long-term maintenance of critical, widely adopted digital infrastructure.
    - Execute coordinated migration waves based on the national dependency and risk roadmap, beginning with high-impact or easily replaceable components.
    - Embed dependency priorities into procurement evaluations and funding decisions.
- Compliance
    - Standardise compliance and licensing processes across PSOs, including SBOM-based monitoring and automated security and licence checks through the social code collaboration platform.
- Measurement
    - Publish annual or biannual OSS metrics reports to national leadership and the OSPO Network.
- Training, Inner Source
    - Institutionalise national training programmes with role-specific pathways, regular updates, and OSPO ambassadors across PSOs.
    - Integrate Inner Source into development routines by requiring PSOs to make internally developed components discoverable and reusable by default unless clear exceptions apply.

7.4.4 Stage 4 – Embedded, resilient, and strategically aligned ecosystem

The purpose of this stage is to realise a stable, sovereign digital ecosystem in which open source, reuse, and shared governance are routine practice, and Denmark actively contributes to European digital commons.

- Policy Strategy
  - Integrate OSS governance across broader national sovereignty domains including AI, cloud, cybersecurity, and data infrastructure.
- Policy Instruments
  - Adopt open-by-default as the standard approach for suitable software development across PSOs, with clear governance, exceptions, and compliance mechanisms.
- Prioritisation & Migration
  - Institutionalise a recurring dependency and risk review cycle (every 2–3 years), updating the migration roadmap and adjusting priorities as technologies, markets, and sovereignty conditions evolve.
- Infrastructure, Stewardship
  - Secure sustained national funding for collaboration platforms, catalogue operations, and stewardship of critical OSS components and dependencies.
- Measurement
  - Maintain continuous evaluation, metrics-driven policy adjustments, and robust stewardship models that ensure resilience beyond organisational or political cycles.

8 Conclusions and future outlook

This study shows that the public sector of Denmark has the building blocks to make OSS a systematic instrument for growing digital sovereignty and promoting innovation and interoperability across its digital infrastructure. Yet, extant assets and capabilities are currently limited, fragmented and unevenly applied or coordinated across actors.

The report proposes a federated support structure that connects national, regional, local, and association-based actors to best enable a comprehensive, collective force to leverage OSS to its fullest. Such a structure can combine policy translation with practical enablement, ensure proximity support for municipalities and PSOs, and make core activities such as stewardship, procurement, compliance and follow-up routine rather than exceptional. With the necessary resourcing, shared collaboration can normalise reuse, strengthen market competition, and grow domestic capability.

The main risks are over-centralisation, fragmentation, and political volatility. These can be mitigated through a clear mandate for a National Government OSPO, along with extended and proximity-based support through a Regional Government OSPO and an Association-based OSPOs that coordinate with the wider ecosystem of regions and municipalities respectively. These are, together with Local Government and Institution-centric OSPOs, organised and coordinated through a national OSPO network with thematic workstreams. Establishing funding programs for innovation and maintenance of OSS solutions in strategic areas is further highlighted as a key enabler for any shift to occur and as a core function within the overarching support structure.

Looking ahead, the commissioning bodies of this report and concerned stakeholders are strongly urged to take a stage-based approach to build the prescribed capabilities, which can be coordinated and leveraged through a systematic, collective approach.

The journey begins with foundational alignment, where a National Government OSPO, a National OSPO Network, prototypes launched, and plans are established for the continued evolution of the support structure. This is followed by a formation phase where a Regional Government OSPO is established to support the Danish Regions, and an Association-based OSPO is formalised through OS2 with its established processes, governance, and ecosystem already in place. The design and operation of the solutions catalogue and social code collaboration platform mature, guidelines and processes for OSS release and intake formalised, along with procurement support, dependency mapping, and funding programmes. This progresses into coordinated scaling, where procurement frameworks embed OSS requirements, compliance becomes standard practice, governance cycles stabilise, and metrics guide policy iteration. In its final stage, the ecosystem becomes embedded and strategically aligned through sustained innovation and maintenance funding, diversified stewardship, alignment with broader sovereignty policies, and active Danish participation in European digital commons.

If these steps are taken, Denmark will move from isolated successes to a durable, scalable ecosystem where open collaboration is the default and sovereignty is a practical property of everyday systems. The result is not more bureaucracy, but better coordination, stronger capabilities, and a public digital infrastructure that is resilient, transparent, and shaped on domestic terms.

9 References

Aarhus Kommune. (2014). *Handlingsplan for open source i Aarhus Kommune: En del af vores it-strategi*. Retrieved December 11, 2023, from https://gambit.aakb.dk/opensource/Handlingsplan_for_OpenSource_i_Aarhus_Kommune.pdf

Advokatfirmaet Poul Schmith. (2020). *Notat vedrørende OS2-fællesskabet og open source*. Retrieved December 11, 2023, from https://opendenmark.dk/wp-content/uploads/2020/06/Notat_endeligt-1.pdf

Alanne, A., Hellsten, P., Pekkola, S., & Saarenpää, I. (2015). Three positives make one negative: Public sector IS procurement. In E. Tambouris et al. (Eds.), *Electronic Government (EGOV 2015)* (Lecture Notes in Computer Science, Vol. 9248). Springer. https://doi.org/10.1007/978-3-319-22479-4_24

Asterès. (2025, April). *Technological dependence on American software and cloud services: An assessment of the economic consequences in Europe* [PDF]. Cigref. https://www.cigref.fr/wp/wp-content/uploads/2025/05/TECHNOLOGICAL-DEPENDENCE-ON-AMERICAN-SOFTWARE-AND-CLOUD-SERVICES-AN-ASSESSMENT-OF-THE-ECONOMIC-CONSEQUENCES.pdf

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security, 31*(3), 337–355.

Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., & Schubert, T. (2021). *The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy* (Final Study Report). European Commission.

Borg, M., Olsson, T., Franke, U., & Assar, S. (2018). Digitalization of Swedish government agencies: A perspective through the lens of a software development census. In *2018 IEEE/ACM 40th International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)* (pp. 37–46). IEEE.

CISA. (2023). *CISA Open Source Software Security Roadmap*. https://www.cisa.gov/sites/default/files/2023-09/CISA-Open-Source-Software-Security-Roadmap-508c%20%281%29.pdf

Computing. (2025, July 8). Denmark's Digital Ministry shifts from Microsoft to LibreOffice in push for digital independence. *Computing*. https://www.computing.co.uk/news/2025/denmark-digital-ministry-drops-microsoft

DIGG – Myndigheten för digital förvaltning. (2025). *Kodsamverkansplattform för öppen programvara i offentlig sektor (Version 1.0)* [Report].

https://github.com/diggsweden/ena-samverkansplattform-os/blob/main/Kodsamverkansplattform_1.0.md

Digitaliseringsstyrelsen. (n.d.). *Signaturprojekter*. https://digst.dk/kunstig-intelligens/signaturprojekter/

Digitaliseringsstyrelsen. (2014). *Open source-software i det offentlige*.

Digitaliseringsstyrelsen. (2022a). *Vejledning om brug af open source i den offentlige sektor*. Retrieved December 6, 2023, from https://arkitektur.digst.dk/node/1173

Digitaliseringsstyrelsen. (2022b). *Vejledning til Statens it-projektmodel*. Retrieved December 8, 2023, from https://digst.dk/media/18239/01-vejledning-til-statens-it-projektmodel-v-13.pdf

Digitaliseringsstyrelsen. (2022c). *Arkitekturregel 2.3: Undgå afhængighed af leverandører og proprietære teknologier*. Retrieved December 8, 2023, from https://arkitektur.digst.dk/node/512

Digitaliseringsstyrelsen. (2024). *Standarder og metoder til krav og anskaffelse*.

Digitaliseringsstyrelsen. (2025). *Open source i den offentlige sektor*. https://digst.dk/media/2zlfki2v/open-source-i-den-offentlige-sektor.pdf

Di Marco, D., Thabit, S., Kotsev, A., Christensen, A., & Minghini, M., et al. (2025). *Open but not powerless: Towards a common understanding of EU digital sovereignty* (JRC144908). European Commission.

Dillon, C., & Litthauer, R. (2020). *Birth of OSPO++: Open Source Program Offices for Governments, Cities and Research Institutions* [Conference presentation]. Linux Foundation Open Source Summit Europe. https://www.youtube.com/watch?v=sPxcpLb2v_4

Direction Interministérielle du Numérique. (2023). *Documentation*. https://code.gouv.fr/documentation/

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. *Research Policy, 52*(6), 104765.

European Commission. (2017a). *Tallinn Declaration on eGovernment*. https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

European Commission. (2017b). *European Interoperability Framework – Implementation Strategy* (COM(2017) 134). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:134:FIN

European Commission. (2020a). *Berlin Declaration on Digital Society and Value-based Digital Government*. https://digital-strategy.ec.europa.eu/en/news/berlin-declaration-digital-society-and-value-based-digital-government

European Commission. (2020b). *Open Source Software Strategy 2020–2023: Think Open*. https://commission.europa.eu/system/files/2023-02/en_ec_open_source_strategy_2020-2023.pdf

European Commission. (2022). *Strasbourg Declaration on the Common values and challenges of European Public Administrations*. https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/new-strasbourg-declaration

European Commission. (2025). *Cloud sovereignty framework* (Version 1.2.1). Directorate-General for Digital Services. https://commission.europa.eu/document/download/09579818-64a6-4dd5-9577-446ab6219113_en

European Commission. (2026, January 12). *Commission opens call for evidence on open-source digital ecosystems*. https://digital-strategy.ec.europa.eu/en/news/commission-opens-call-evidence-open-source-digital-ecosystems

European Parliament. (2026, January 22). *European technological sovereignty and digital infrastructure* (2025/2007(INI)). https://www.europarl.europa.eu/doceo/document/TA-9-2026-0022_EN.pdf

Færdselsstyrelsen. (2025). *Færdselsstyrelsen tager første skridt mod open source-pc'er i staten*. https://www.fstyr.dk/nyheder/2025/dec/faerdselsstyrelsen-tager-foerste-skridt-mod-open-source-pc'er-i-staten

Frey, R. (2023). How we lead successful open-source collaborations in the Danish public sector. *IEEE Software, 40*(4), 19–24.

Folketinget. (2025, April 23). *DIU høring digital suverænitet*. https://www.ft.dk/da/aktuelt/nyheder/2025/04/diu-hoering-digital-suveraenitet

Foundation for Public Code. (2023). *Standard for Public Code*. https://standard.publiccode.net/

Germonprez, M., & Linåker, J. (2024). Measuring and communicating impact by your OSPO. In *The Open Source (Program) Office Book*. TODO Group / Linux Foundation.

GitHub. (n.d.). *GitHub and government: Who is using GitHub?* Retrieved December 20, 2023, from https://government.github.com/community/

Government Digital Service. (2017). *Government service design manual: Making source code open and reusable*. https://www.gov.uk/service-manual/technology/making-source-code-open-and-reusable

Government Digital Service. (2022). *Service Standard*. https://www.gov.uk/service-manual/service-standard

Haddad, I. (2020). *A close look at Open Source Program Offices: Structure, roles and responsibilities*. https://github.com/ibrahimhaddad/publications/blob/master/Open%20Source%20Program%20Offices.pdf

Herpig, S. (2023). *Government cybersecurity Open Source Program Office*. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/snv_fostering_open_source_software_security.pdf

Interoperable Europe. (2025, June 17). *Aarhus and Copenhagen choose open source.* https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/aarhus-and-copenhagen-choose-open-source

Kommunernes Landsforening. (n.d.). *Kriterier for den fælleskommunale rammearkitektur*. Retrieved December 14, 2023, from https://rammearkitektur.kl.dk/

Kommunernes Landsforening. (2023). *Den gode it-anskaffelse*. Retrieved December 12, 2023, from https://videncenter.kl.dk/viden-og-vaerktoejer/

Kommunernes Landsforening. (2025a). Aftale om tre storskalaprojekter med kunstig intelligens i den offentlige sektor. https://www.kl.dk/forsidenyheder/2025/december/aftale-om-tre-storskalaprojekter-med-kunstig-intelligens-i-den-offentlige-sektor

Kommunernes Landsforening. (2025b). Kommunernes skaleringssamarbejde. https://videncenter.kl.dk/videncenter/viden-og-vaerktoejer/velfaerdsteknologi/kommunernes-skaleringssamarbejde

KOMBIT. (n.d.). *Digitaliseringskataloget*. https://digitaliseringskataloget.dk/

Kummer, C. (2025, June 18). Aarhus and Copenhagen choose open source. *Interoperable Europe Portal.* https://interoperable-europe.ec.europa.eu/collection/open-source-observatory-osor/news/aarhus-and-copenhagen-choose-open-source

Laursen, J. (2025, October 22). Aarhus udfaser Microsoft-pakken. *HK Kommunal.* https://www.hk.dk/aktuelt/nyheder/2025/10/22/aarhus-udfaser-microsoftpakken

Linåker, J., & Regnell, B. (2020). What to share, when, and where: Balancing the objectives and complexities of open source software contributions. *Empirical Software Engineering, 25*, 3799–3840.

Linåker, J., Nummelin Carlberg, A., & O'Riordan, C. (2024). *Public Sector Open Source Program Offices - Archetypes for how to Grow (Common) Institutional Capabilities*. European Commission, DIGIT. https://arxiv.org/pdf/2603.04891

Linåker, J., & Muto, S. (2024). *Software reuse through open source software in the public sector: A qualitative survey on policy and practice*. RISE Research Institutes of Sweden.

Linåker, J., Link, G., & Lumbard, K. (2024). Sustaining maintenance labour for healthy open source software projects through human infrastructure. In *18th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*.

Linåker, J., Gates, N., Chourmouziadis, Y., & Weber, S. (2025a). *Open source software adoption and reuse in European local governments*. European Commission, DIGIT.

Linåker, J., Lundell, B., Servant, F., Gamalielsson, J., Muto, S., & Robles, G. (2025b). Public sector open source software projects: How is development organised? *Empirical Software Engineering, 30*(3), 1–54.

Lundell, B., Gamalielsson, J., Butler, S., Brax, C., Persson, T., Mattsson, A., & Öberg, J. (2021a). Enabling OSS usage through procurement projects: How can lock-in effects be avoided? In *IFIP International Conference on Open Source Systems* (pp. 16–27). Springer.

Lundell, B., Gamalielsson, J., Katz, A., & Lindroth, M. (2021b). Perceived and actual lock-in effects amongst Swedish public sector organisations when using a SaaS solution. In *International Conference on Electronic Government* (pp. 59–72). Springer.

Marco-Simó, J. M., & Pastor-Collado, J. (2020). IT outsourcing in the public sector: A descriptive framework from a literature review. *Journal of Global Information Technology Management, 23*(1), 25–52.

Mikalsen, M., & Farshchian, B. (2020). Can the public sector and vendors digitically transform? A case from innovative public procurement. *ECIS Research-in-Progress Papers*, 62.

Mission Bothorel. (2021). *Pour une politique publique de la donnée*. French Ministry of Economy. https://www.mission-open-data.fr

Mygind, D. (2008). Gode råd: Sådan bruges open source i det offentlige. *Computerworld*. Retrieved December 12, 2023, from https://www.computerworld.dk/art/44741/

Nagle, F. (2022). *Strengthening digital infrastructure: A policy agenda for free and open source software*. Brookings Institute.

Nagle, F. (2023). Government IT procurement policy & firm behavior: Evidence from a French OSS policy. *Academy of Management Proceedings, 2023*(1), Article 13046.

New Zealand Government. (2016). *NZGOAL software extension policy* (Version 1). https://www.data.govt.nz/toolkit/policies/nzgoal/nzgoal-se/

OpenForum Europe. (2022a). *The OSPO: A new tool for digital government*. https://openforumeurope.org/publications/the-ospo-a-new-tool-for-digital-government/

OpenForum Europe. (2022b). *Open strategic autonomy: Ensuring Europe's access to key enabling technologies*. https://openforumeurope.org/

Open Source Business Alliance. (2025). *Selection criteria for the sustainable procurement of open source software: Position paper*. https://osb-alliance.de/

Open Source Observatory and Repository. (2012). *The best software for the purpose: softwarebørsen.dk*. https://joinup.ec.europa.eu/

OS2. (2017). *Open source anskaffelse – Licenser, jura, udbud og kontrakter*. https://faq.os2.eu/

OS2. (n.d.). *Open source produkter i OS2-fællesskabet*. https://www.os2.eu/os2-it-loesninger

OS2. (2025, December 3). *OS2skole – en ny digital platform*. https://boks.os2.eu/

OSPO Alliance. (2021). *OSPO Alliance Position Paper*. https://ospo.zone/docs/

PA Consulting. (2026, January). *Digital suverænitet i den offentlige sektor: Sammenfattende analyse*. KL. https://www.kl.dk/

Persson, P., & Linåker, J. (2024). Soft-lockins in public sector acquisitions of open source software solutions: A case study. In *Proceedings of HICSS-58*.

Procee, R., Al-Saqaf, M., Spanninga, H., Vos, F., & van der Meer, H. (2022). *Opensourcewerken: De vrijblijvendheid voorbij*. Ministry of the Interior. https://open.overheid.nl/

PwC. (2019). *Strategische Marktanalyse zur Reduzierung von Abhängigkeiten*. Bundesministerium des Innern. https://www.wibe.de/

Regeringen, KL, & Danske Regioner. (2025). *Den fællesoffentlige digitaliseringsstrategi 2026–2029*. Digitaliseringsstyrelsen. https://digst.dk/

Ruff, N. (2022). The rise of the Open Source Program Offices (OSPO). In A. Brock (Ed.), *Open source law, policy and practice*. Oxford University Press.

SKI. (n.d.). *02.06 Aftalegrundlag, Dynamisk indkøbssystem (17090)*. Retrieved December 2, 2025, from https://www.ski.dk/

Sørensen, H. K. (2025, December 16). Styrelse vil være uafhængig af Microsoft. *DR Nyheder*. https://www.dr.dk/

TechCity Aarhus. (2025, August 19). Aarhus Municipality develops its own AI assistant. *TechCity Aarhus*. https://techcityaarhus.com/

Teknologirådet. (2002). *Open source software i den digitale forvaltning: Analyse og anbefalinger*. Retrieved December 11, 2023, from http://webhotel4.ruc.dk/

The TODO Group. (2022a). *Open Source Program Office (OSPO) definition and guide*. https://github.com/

The TODO Group. (2022b). *Announcing OSPO Survey 2022 results*. https://todogroup.org/

TODO Group. (2024). *Role classifications in OSPOs*. https://todogroup.org/

TODO Group. (2025). *Chapter 3: Creating your OSPO*. In *OSPO Book*. https://ospobook.todogroup.org/

von der Leyen, U. (2026, January 20). *Special address at the World Economic Forum* (SPEECH_26_150). European Commission. https://ec.europa.eu/

Wet open overheid. (2023). https://wetten.overheid.nl/BWBR0045754/

Wright, N. L., Nagle, F., & Greenstein, S. (2023). Open source software and global entrepreneurship. *Research Policy, 52*(9), 104846.

Zentrum für Digitale Souveränität der Öffentlichen Verwaltung. (2024). *Stellungnahme „Open Source“ im Ausschuss für Digitales des Deutschen Bundestags*. https://www.zendis.de/

10 Annex A – Interviewee and workshop participant demographics

Table 2: List of participants in interviews and workshops.

Name	Role	Organisation
Rasmus Frey	Sekretariatschef	OS2
Jacob Andersen	Senior Software/ICT Engineer	Alexandra Instituttet
Martin Wood	IT-direktør	Domstolsstyrelsen
Martin Buur	Enhedschef	Domstolsstyrelsen
Thor Schliemann	IT-arkitekt	Digitaliseringsstyrelsen
Nikolai Bülow Tronche	Kontorchef i Kontor for teknologi og data	Digitaliseringsstyrelsen
Christian Boesgaard,	Udviklingschef	DBC Digital
Peder Wiese	CTO	Statens IT
Jakob Eiby	IT-arkitekt	KL
Line Laudrup	Chefkonsulent	KL
Lars Vraa	Chef for Design & Arkitektur	KOMBIT
Allan Schiellerup Bager	Chefkonsulent	SKI
Asbjørn William Ammitzbøll Flügge	Chefkonsulent	IT-Branchen
Ole Tange	IT-politisk rådgiver	Prosa
Morten Kjærsgaard	Direktør/formand	Magenta/DOSL
Bo Fristed	Digitaliseringschef	Aarhus Kommune
Jens Kjellerup Hansen	Chefkonsulent	Ballerup Kommune

Name	Role	Organisation
Henrik Hammer Jordt	Chefarkitekt/formand	Region Midtjylland/Regionernes It-Arkitekturråd (RITA)
Marie Gottlieb Danneskiold-Samsøe	Stabschef	Ringsted Kommune
Karen Melchior	Senior Advisor	CEPS (Centre for European Policy Studies)
Gina Plat	OSPO BZK Programma Manager	I-Interim Rijk - Dutch National Government OSPO
Lea Beiermann	Partnership lead	ZenDIS, German national government OSPO
Alexander Rosenthal	Manager, DigitalHub.SH	WTSH GmbH - Schleswig-Holstein Regional Government OSPO
Nicole Beckendorf	Head of OSPO	Land Schleswig-Holstein - Schleswig-Holstein Regional Government OSPO
Tony Shannon	Head of Digital Services	Office of Government Chief Information Officer at Department of Public Expenditure & Reform, Ireland
Evans Ikua	Head of OSPO	Incubating UNDP OSPO of Kenya
Bevan Agard	Head of OSPO	Incubating UNDP OSPO of Trinidad & Tobago
Himal Mandalia	Independent consultant	Former Head of Technology for GOV.UK, Consultant to UNDP Digital, AI and Innovation Hub on digital capability, OSPO readiness, and DPI advisory.

11 Annex B – Interview questionnaire

11.1 Introduction and background

(Purpose: establish context and rapport)

- Can you describe your role and how it connects to digitalization or software development within your organization?
- What experiences has your organization had with open source software (OSS) so far, either using, developing, or sharing it?
- How would you describe the general perception and awareness of OSS within your organization or among your peers?

11.2 Strategic goals and vision (RQ1)

(Exploring alignment with digital strategies and autonomy goals)

- From your perspective, what should be Denmark's main strategic goals regarding the use and reuse of OSS in the public sector?
- How do you see OSS contributing to broader policy goals such as openness, interoperability, or digital sovereignty?
- Are there incentives that could motivate your organization to participate more actively in OSS initiatives?
- How do you think OSS aligns (or conflicts) with existing digitalization strategies or political priorities?

11.3 Barriers and challenges (RQ2)

(Exploring obstacles to OSS collaboration and reuse)

- What are the main barriers your organization faces when trying to adopt or reuse OSS from other public-sector bodies, or from OSS in general?
- How do procurement rules or risk considerations affect your ability to share or reuse OSS?
- To what extent do you find that organizational culture or leadership attitudes hinder OSS adoption or collaboration across agencies?
- Are there any technical, legal, or knowledge-related obstacles that you think are particularly limiting?

11.4 Capabilities required (RQ3)

(Focusing on competencies, structures, and processes)

- What skills or competencies do public organizations need to effectively develop, share, and reuse OSS?
- Does your organization have internal teams or units equipped to manage OSS governance, compliance, or community engagement?

- How do you think public-sector entities can build or strengthen such capabilities – through training, shared frameworks, or external support?

11.5 Existing actors and frameworks (RQ4)

(Identifying current supports and gaps)

- Which national or sectoral actors (e.g., OS2, Agency for Digital Government, Local Government Denmark) do you see as most supportive for OSS collaboration?
- Are there particular policies, catalogues, or initiatives that already facilitate OSS sharing or reuse?
- What types of support or frameworks are currently missing to help organizations use OSS more systematically?
- Have you interacted with networks, communities, or associations that promote OSS collaboration among municipalities or government bodies?

11.6 Realization through OSPOs (RQ5)

(Design-oriented and solution-building questions)

- How familiar are you with the concept of an Open Source Program Office (OSPO)?
- In your view, what functions should a national or cross-government OSPO include to support reuse and collaboration among PSOs?
- Should such an OSPO focus more on technical assistance, legal guidance, capability-building, or coordination?
- How might existing institutions like OS2 or the Agency for Digital Government contribute to or host such an OSPO?
- What do you think should be avoided when designing an OSPO for the Danish public sector?

11.7 Reflections and outlook

(Closing and reflective questions)

- Looking forward, what changes would most help your organization, and the Danish public sector overall, build a stronger open source ecosystem?
- Is there a successful initiative (in Denmark or abroad) you believe could serve as a model for strengthening OSS reuse in public administration? (RQ5)
- Do you have any final reflections or suggestions on how collaboration on OSS could be improved nationally?

Through our international collaboration programmes with academia, industry, and the public sector, we ensure the competitiveness of the Swedish business community on an international level and contribute to a sustainable society. Our 2,800 employees support and promote all manner of innovative processes, and our roughly 100 testbeds and demonstration facilities are instrumental in developing the futureproofing of products, technologies, and services. RISE Research Institutes of Sweden is fully owned by the Swedish state.

I internationell samverkan med akademi, näringsliv och offentlig sektor bidrar vi till ett konkurrenskraftigt näringsliv och ett hållbart samhälle. RISE 2 800 medarbetare driver och stöder alla typer av innovationsprocesser. Vi erbjuder ett 100-tal test- och demonstrationsmiljöer för framtidssäkra produkter, tekniker och tjänster. RISE Research Institutes of Sweden ägs av svenska staten.

RISE Research Institutes of Sweden AB
Box 857, 501 15 BORÅS, SWEDEN
Telephone: +46 10-516 50 00
E-mail: info@ri.se, Internet: www.ri.se

RISE Report 2026:38
ISBN: 978-91-90109-67-0

A report commissioned by the Danish Agency for Digital Government (Digitaliseringsstyrelsen) and Local Government Denmark (KL)

RISE – Research Institutes of Sweden
ri.se / info@ri.se / 010-516 50 00
Box 857, 501 15 BORÅS

Grants Office/Informationscenter
RISE Rapport: 2026:38
ISBN: 978-91-90109-67-0