CADA – vragenlijst open consultatie voor overheden

Dit document is bedoeld voor de interdepartementale beantwoording van de open consultatie van de Cloud & AI Development Act (CADA). De consultatie kent meerdere secties, waarvan er twee specifiek relevant zijn voor input vanuit de rijksoverheid:

- Sectie 2.5 biedt de mogelijkheid te reageren vanuit de overheid als gebruiker van AI en clouddiensten.
- Sectie 3 biedt de mogelijkheid te reageren vanuit de beleidsverantwoordelijkheid op het vlak van AI, clouddiensten en datacenters.

In het vervolg van dit document zijn de vragen uit de consultatie en beantwoording hiervan uit die twee secties uiteengezet. De beantwoording van multiple choice vragen zijn **dikgedrukt** en met een 'X' aangegeven en antwoorden van open vragen zijn *schuingedrukt.*

Section 2.5: Questions of Public Administrations

Q1: On behalf of what type of public administration are you answering?
Answer: Local/Regional/**National**/Federal/European

2.5.1 Current situation

Q2: Does your public administration currently use cloud computing and AI services?
Answer: **Yes**/No/I don't know

Q3: What types of cloud services do you use?
Answer (multiple possible):

- **X Infrastructure as a Service - IaaS (e.g. Virtual Machines, storage, infrastructure)**
- **X Platform as a Service – PaaS**
- **X Software as a Service – SaaS**
- Other (please specify, max. 1000 characters)
- I don't know

Q4: Do you store data on the cloud?
Answer: **Yes/**No, only on-premises/I don't know

Q5: What type of data do you store in the cloud? (PM BZK)
Answer (multiple possible):

- Sensitive information, such as data related to public security or public safety
- Special categories of sensitive data such as health records or financial data
- Other data that my organisation considers sensitive (if so, please specify)
- Commercially sensitive data, including data subject to intellectual property rights as well as trade secrets
- Operational data related to functioning of digital public services
- Public data
- Open data
- Trained AI models
- Other (please specify, max. 1000 characters)

Q6: How do you store this data on the cloud?
Answers: All encrypted/All non-encrypted/**It depends on the data classification and sensitivity**/I do not know

Q7: Please specify the data classification and sensitivity
Answer: *4000 character(s) maximum*

There are 3 classifications namely: 1. Unclass, 2. Restricted and/or 3. higher. Within unclass there are numerous specific markings applicable which make the data more or less sensitive, compliant with National, European and NATO information security policies.

Q8: When selecting cloud providers for your organisation how concerned are you with respect to the following:
Rank each answer on a scale from 1 to 5, where 1 = not concerned at all and 5 = very concerned

	1	2	3	4	5	Not applicable / I don't know
* Sensitive data of your organisation is accessed by authorities of a third country in circumvention of applicable EU laws and regulations (e.g. GDRP, Data Act)					X	
*Cloud provider is headquartered in a third country that poses specific cyber-security threats to the Union					X	
* Risks such as undue influence by a third country on suppliers and service providers, in particular in the case of alternative models of governance; concealed vulnerabilities or backdoors; and potential systemic supply disruptions, in particular in the case of technological lock-in or provider dependency					X	
*Other (please specify, max. 4000 characters)						

Q9: Which cloud deployment model(s) does your public administration rely on?
Answer (multiple possible):

- **X Government private cloud**
- **X Public cloud**
- **X Hybrid cloud**
- **X Other (please specify, max. 1000 characters)**

Multi cloud (using multiple (commercial) parties together to run services), and traditional data centers.

- I don't know

Q10: Are any of your procured providers subject to non-EU jurisdictions including laws with extraterritorial effect (e.g. US or Chinese providers)?
Answer: **Yes**/No/I don't know

Q11: What are the main factors driving the decision of which cloud service will be procured in your administration?
Rank each answer on a scale from 1 to 5, where 1 = not very important and 5 = very important

Factor	1	2	3	4	5	Not applicable / I don't know
*Level of assurance and protection, i.e. the security mechanisms put in place depending on the sensitivity of the data					X	
*Price			X			

*Made in Europe			X			Def: increasing in importance
*Provenance of the provider				X		
*Integration with other services from the same provider, for instance, software tools			X			
*Integration with other services from other providers			X			
*Interoperability with other providers					X	
*Integrated offerings (bundle)			X			
*Sustainability				X		
*Latency			X			
*Reliability				X		
*Scalability				X		
*Other (please specify, max. 4000 characters)						

Q12: What are the main reasons for not using cloud computing by your administration?
Rank each answer on a scale from 1 to 5, where 1 = not very important and 5 = very important

Reason	1	2	3	4	5	Not applicable / I don't know
*Total Cost of Ownership		X				
*Not enough knowledge to select the most appropriate service for different data sensitivities		X				
*Cybersecurity				X		
*Data protection concerns					X	
*Limited knowledge or lack of expertise in operation and management of cloud services (e.g. in terms of technical, administrative capabilities)				X		
*Limited offering from EU providers			X			
*Compliance with EU regulations (e.g. GDPR, Data Act)					X	
*Risk of unlawful access to data from third countries legislation with extra territorial reach					X	
*Fear of vendor lock in				X		
*Fear of interoperability issues				X		
*High operational cost of migration from on-premise solutions			X			
*Sustainability concerns		X				

*Preference/ No need				X		
*Other (please specify, max. 4000 characters)						

Q13: Is the software developed in your public administrations released as open source software?
Answer: Yes/**No**/I don't know

Q14: Is there an established public repository where the code can be accessed and contributed to?
Answer: **Yes**/No/I don't know

Q15: Is there a community governance mechanism put in place for the code released as open source?
Answer: Yes/**No**/I don't know

2.5.2 Specific needs and challenges

Q16: What are your administration's top priorities when using cloud computing?
Rank each answer on a scale from 1 to 5 where 1 = not very important and 5 = very important

Priority	1	2	3	4	5	Not applicable / I don't know
*Scalability				X		
*Cost efficiency			X			
*Risk of unlawful access to data from actors subject to non-EU legislation with extraterritorial reach					X	
*Security mechanisms in place					X	
*Data protection measures					X	
*Availability / Uptime				X		
*Performance				X		
*Integration with other services from the same provider, for instance, software tools			X			
*Integration with other services from other providers			X			
*Interoperability with other providers					X	
*Integrated offering (bundle)		X				
*Made in Europe				X		
*Environmental sustainability				X		
*Protection from cybersecurity risks posed by certain countries					X	
*Other (please specify, max. 4000 characters)						

Q17: What challenges have you encountered with the adoption of cloud by your administration?
Rank each answer on a scale from 1 to 5, where 1 = not very important and 5 = very important

Challenge	1	2	3	4	5	Not applicable / I don't know
*Limited knowledge on how to technically evaluate, assess and procure the existing cloud service offerings			X			
*Security risks				X		
*Vendor lock in				X		
*Limited technical expertise					X	
*Limited or lack of interoperability				X		
*Regulatory, including public procurement requirements				X		
*Other (please specify, max. 4000 characters)						

Q18: Are there any gaps in the current offerings of cloud computing providers that impact your operations?
Answer: *4000 character(s) maximum*

The lack of European Cloud providers who can provide their services at scale limits our ability to switch to their cloud offerings in full.

Q19: How can the EU support public administrations in increasing their use of cloud computing?
Rank each answer on a scale from 1 to 5, where 1 = not very important and 5 = very important

Factor	1	2	3	4	5	Not applicable / I don't know
*Funding			X			
*EU-wide uniform guidance on how to procure			X			
*Mechanisms to allow federation of cloud services across public administrations within and across Member States					X	
*Standards, open specifications and mechanisms to ensure interoperability of cloud solutions				X		
*Cybersecurity guidelines				X		
*Technical support, training and capacity building support			X			
*Other (please specify, max. 4000 characters) • *Considering public administrations as a strategic use case for cloud technologies, in order to attract innovation and investment opportunities for this specific and sensitive use of cloud.*					X	

• *Develop a common definition with criteria on cloud sovereignty, such as clarity on the use of sovereign and not-sovereign cloud, access to and ownership of data, and clarity on exclusive EU or member states jurisdiction for EU based cloud infrastructures.* • *Develop a common risk assessment to provide guidance to member states in making well-considered choices on the use of cloud (including minimum standards and common levels on security, privacy and sovereignty).* • *Provide more possibilities in public procurement directives to limit the risks to (national) security, to steer more on strengthening sovereignty and to guarantee the continuity of government services.* • *Separately, Cybersecurity certification based upon Cybersecurity certification schemes under the CSA (Cybersecurity Act) focusing on proven levels of cybersecurity. Finalize EUCS as soon as possible and integrate that in procurement requirements.*						

Q20: Does your administration release the code procured for the delivery of digital services as open source?
Answer: Always/**In some cases**/Never/I don't know/Not applicable

Q21: Is there any licensing schema preferred? (PM BZK)
Answer: *4000 character(s) maximum*

Q22: What is preventing you from this?(PM BZK)
Answer (multiple possible):
- Licenses
- Cybersecurity vulnerabilities
- Maintenance
- Sustainability
- Accountability
- Other (please specify, max. 1000 characters)

Q23: Are there any specific policy measures you would recommend to improve public administrations' access to and use of cloud services?
Answer: *4000 character(s) maximum*

Public administrations possess and use a lot of critical and sensitive data. Policy measures on improving the access and use of cloud services should therefore primarily focus on making well-considered decisions on the access and use of different types of (public) cloud technologies instead of focusing on the aim to make more use of cloud technologies in general.

Policy measures could include:
- Providing guidance by developing a common risk assessments on the use of public cloud technologies. This risk assessment should be combined with common minimum standards for the different types of cloud applications in order to ensure common levels of security, privacy, and

sovereignty.
- Supporting the use of open standards and solutions with the aim to optimise the freedom of choice, improve interoperability and reduce vendor lock-in.
- Develop a common definition with criteria on cloud sovereignty. This is necessary to reduce the vast grey zone between sovereign and not-sovereign cloud and it will form the basis for collective European action in this field. This definition should entail the following criteria: clarity on the use of sovereign and not-sovereign cloud, access to and ownership of data, and clarity on exclusive EU or member states jurisdiction for EU based cloud infrastructures.

- Ensure transparency from cloud service providers regarding the location of data (including telemetry and diagnostics) and services, as well as the relevant jurisdictions. This transparency should extend to the necessary sub-services utilized by cloud providers to deliver their services to customers.
- Provide financial instruments for innovation and use of critical cloud technologies by public administrations, for example under the current Digital Europe Programme (DEP) and Connecting Europe Facility (CEF Digital). Besides, it is of importance that cloud technologies (used by public administrations) form part of a limited set of digital technologies for investments under the next Multi-annual Financial Framework (MFF).
- To use the strength of public administrations in public procurement in order to accelerate investments in the development and scaling of cloud applications for the most essential and critical cloud solutions used in public administrations.

Q24: Are there any specific policy measures you would recommend for the provision of the security of cloud services for public administrations?
Answer: *4000 character(s) maximum*
- Develop common minimum standards for the different types of cloud applications in order to ensure common levels of security, privacy, and sovereignty.
- Develop a common definition with criteria on cloud sovereignty. This is necessary to reduce the vast grey zone between sovereign and not-sovereign cloud and it will form the basis for collective European action in this field. This definition should entail the following criteria: clarity on the use of sovereign and not-sovereign cloud, access to and ownership of data, and clarity on exclusive EU or member states jurisdiction for EU based cloud infrastructures.
- The revision of the public procurement directives should include more possibilities to limit the risks to (national) security, to steer more on strengthening sovereignty and to guarantee the continuity of government services.

Section 3: EU Policies - 3.1 Computing Capacities

Q1: What type of EU action should be prioritised for boosting the availability of sufficient and adequate cloud capacity for AI workloads?
Rank each answer on a scale from 1 to 5, where 1 = not very relevant and 5 = very relevant

1a: Facilitation of investment

Policy action	1	2	3	4	5	Not applicable / I don't know
*Increasing public investment into private public infrastructures		X				
*Creating public private partnerships for large scale data centres		X				
*Incentives for building computing infrastructure in underserved regions		X				
*Other (please specify, max. 4000 characters) - Investments in specific cloud services which are currently not provided by European companies and more support for initiatives to support integration of services from different service providers					X	
-Focus on conditions that are critical for creating cloud portability and avoid vendor lockins. E.g. Limit modification of open source implementations as much as possible to improve portability of services / Control options for CSC's regarding identities and encryption of data (transmit / storage)				X		
-Focus on addressing opportunities in Cloud developments as pre conditional to be future resistant and optimise usage for AI systems. E,g, microservice architecture / multicloud implementations / 5G integration of cloud services				X		
-Facilitate SME acces to cloud and AI infrastructure.				X		

1b: Simplification of infrastructure permitting procedures

Policy action	1	2	3	4	5	Not applicable / I don't know
*Have a one stop shop service or a similar mechanism where the different permits at the different administrative levels can be requested and managed	X					
*Reduce the amount of time necessary to obtain the different certificates and permissions			X			

*Create expedited approval mechanisms and clear conditions for critical / strategic projects	X					
*Other (please specify, max. 4000 characters)		X				

1c: Simplification of regulations for the building of computing infrastructure with energy efficiency

Policy action	1	2	3	4	5	Not applicable / I don't know
*Unified guidelines at national level for all aspects including energy efficiency	X					
*Unified guidelines at EU level				X		
*Other (please specify, max. 4000 characters) *Provide standards addressing the measurement of parameters relevant for identifying efficiency in energy. Refer from implementing additional Regulation on energy efficiency. Set up a reporting system to provide transparency which could include a Marking schedule to encourage efficiency.*			X			

1d: Environmental aspects

Policy action	1	2	3	4	5	Not applicable / I don't know
*Clear environmental compliance requirements					X	
*Addressing energy availability for data centres					X	
*Addressing land availability for data centres		X				
*Other (please specify, max. 4000 characters) *Clear requirements on additional sustainability efforts such as Capturing Heat from data centers.*				X		

1e: Energy efficiency

Policy action	1	2	3	4	5	Not applicable / I don't know
*Tax incentives for using sustainable technologies				X		
*Funding for research and development of energy-efficient technologies				X		
*Standardized energy efficiency benchmarks					X	

*Investments in the development of more efficient software to manage and monitor the energy efficiency and metrics of the data centre				X		
*Other (please specify, max. 4000 characters)						

1f: Cross-cutting issues

Policy action	1	2	3	4	5	Not applicable / I don't know
*Supporting an open source software ecosystem				X		
*Collaborative programs for R&D and innovation					X	
*Other (please specify, max. 4000 characters) In the AI Continent Action Plan, it is suggested that the CADA should also contribute to establishing a common EU marketplace for cloud capacity and services to enable the entry into the market of a more diverse set of cloud service providers. In our view, this should be a central objective of the Act.					X	

Q2: At EU policy level, is it appropriate to distinguish between capacity for training, for fine-tuning, and for inference of AI models and solutions?
Answer: **Yes**/No/I don't know (if No, please specify)

3.2 Public Sector actions

Q3: What EU policy actions would best address the current issues faced by Public Administrations when procuring cloud and AI services?
Answer (multiple possible):

- **X Guidelines with standard criteria to procure cloud services**
- **X Guidelines with standard award criteria**
- **X Standardized tender vocabulary and requirements**
- I don't know
- **Other (please specify, max. 1000 characters)**

Referencing EUCS as applicable cybersecurity certification and give the issuance of EUCS top priority to gain a higher cybersecurity level EU wide at short notice.

Q4: What EU policy actions would address the current issues faced by Public Administrations on cloud and AI services?
Answer (multiple possible):

- **X Include a criterion ensuring sovereignty, autonomy, resilience and availability in the procurement of narrowly defined highly critical and strategic use cases**
- Include a criterion for highly innovative solutions
- Include a criterion for solutions with added value and innovation
- **X Improvement of skills and capabilities, including training and certifications**
- Marketplace of cloud services, AI services, and other software applications for the Public sector.
- **X Other (please specify, max. 4000 characters)**

-Include a criterion for platform independent cloud and AI hosting ensuring application and data portability

-Encourage using Opensource and EU options

-Provide funding or incentives for open-source compliance-as-code for public institutions that want to make use of EU Cloud providers, i.e. open-source reference architectures and template code implementations that convert information security frameworks or directives (e.g. ISO:27001, NIS2, NL-BIO, Spain ENS) into starting points for policy-as-code technical security controls that are easy and straightforward to implement. For The Netherlands the Microsoft Azure BIO compliancy policies and for Spain ENS technical Azure controls are deployable with a single mouse click. This considerably speeds up compliance for public organisations as foundation for security and compliance. Similar starting points with relevant policy-as-code repositories for information security compliance are absent for European Cloud providers. These kinds of practical common baselines help both EU cloud providers as well as public institutions achieve better and faster adoption.

Optimize the use of EUCS certification for addressing cybersecurity issues. So prioritize the initiation of EIUCS for the short term. Thus limiting the necessity of having a wide range of Assurance reports / certification that even might be member state specific. With one certification addressing all cybersecurity criteria.

- ☐ I don't know

3.3. Open source in the public sector

Q5: What EU policies would alleviate the challenges of releasing the code funded by public money as open-source* code?
**released under a license in which the copyright holder grants users the rights to use, study, change, and distribute the software and its source code to anyone and for any purpose.*
Answer (multiple possible):

- ☐ **X A common open-source licensing schema across the EU**
- ☐ **X Guidelines to set up the governance mechanisms of the open-source community**
- ☐ **X Guidelines to select relevant open-source communities/foundations where the code can be released**
- ☐ **X The set up of a public-private foundation dedicated to such communities**
- ☐ **X An obligation to release the source code developed with public money onto open-source repositories, except in duly justified cases**
- ☐ Other (please specify, max. 4000 characters)

Development of a licensing schema that permits the use of open-source code developed with public funds for EU entities.

Funding for maintenance of open-source code.

- ☐ I don't know

3.4 Cross-cutting topics

Q6: What EU policy actions would address bundling?
Bundling is a commercial strategy where several software packages are sold together for distribution, deployment or use.
Answer (multiple possible):

- Regulation of bundling practices to ensure fair competition
- **X Promoting open licensing models for AI tools and platforms**
- **X Transparency requirements for cloud provider pricing and licensing**
- I don't know
- Other (please specify, max. 4000 characters)

Transparency requirements for addressing user entity controls involved in these kind of bundling activities. Transparency about how cybersecurity is addressed in the bundle.

Q7: What EU policy action would best serve to protect against unlawful access to [sensitive] data [by third-country legislation with extraterritorial reach] and risks associated with supply chain dependencies and possible disruptions) of cloud and AI services?
Answer (multiple possible):

- **X Pursue international cooperation (including international agreement) with third countries that address such risks**
- Develop criteria that could be used to differentiate between third countries depending on whether they pose specific threats to the Union.
- **Develop criteria to narrowly identify highly critical use cases for cloud and AI services**
- **Define criteria to narrowly identify highly critical use cases for which public procurers could address specific risks related to third countries' legislation with extraterritorial reach, aligned with international agreements.**
- Other (please specify, max. 4000 characters)
- I don't know

Q8: *The EU pursues and has concluded with third countries agreements facilitating trusted cross-border data flows and prohibiting unjustified data localisation restrictions, including with the UK, Japan, Singapore and Korea.* **How important is it in your view that the EU promotes such partnerships with likeminded countries?**
Answer: **Very important**/Somewhat important/Neutral/Not very important/Not important at all