Contribution ID: 997fa312-4d4e-4001-aff1-0d28b582138f
Date: 03/07/2025 14:07:38

Open Public consultation questionnaire on the proposal for a Cloud and AI Development Act

Fields marked with * are mandatory.

Introduction

This consultation on the Cloud and AI Development Act is structured along three sections:

Section 1: General questions for all respondents
This section includes a set of general questions applicable to all respondents. Your responses here will guide which subsequent questions you receive in Section 2, based on your stakeholder category.

Section 2: Stakeholder-Specific Questions
To tailor the consultation to your area of expertise, please begin by selecting "I am giving my contribution as" to identify your stakeholder category.

To begin, please choose "I am giving my contribution as" to select your specific stakeholder category. You can choose from the following:

- Public Administrations
- Citizens
- NGOs
- Academic/Research Institutions
- Business Associations
- Consumer Organisations
- Environmental Organisations
- Trade Unions
- Company/Business

If you select "Company/Business," please specify further as follows:

- Data Centre Operators
- Cloud / Telco / Edge Providers
- AI Developers and Providers
- Cloud / Edge / AI Users
- Financial Institution, Investor, Fund

Your selection will help us direct you to the relevant questions for your category, ensuring a more focused and effective consultation.

Section 3: EU Policy
In the final section, all participants are asked to share their views on potential policies to be adopted on cloud policy.

About you

* First name

* Surname

* Email (this won't be published)

* Language of my contribution

- Bulgarian
- Croatian
- Czech
- Danish
- Dutch
- English
- Estonian
- Finnish
- French
- German
- Greek
- Hungarian
- Irish
- Italian
- Latvian
- Lithuanian
- Maltese

- Polish
- Portuguese
- Romanian
- Slovak
- Slovenian
- Spanish
- Swedish

* I am giving my contribution as
  - Academic/research institution
  - Business association
  - Company/business
  - Consumer organisation
  - EU citizen
  - Environmental organisation
  - Non-EU citizen
  - Non-governmental organisation (NGO)
  - (•) Public authority
  - Trade union
  - Other

* Organisation name

255 character(s) maximum

The Government of The Netherlands

* Organisation size
  - Micro (1 to 9 employees)
  - Small (10 to 49 employees)
  - Medium (50 to 249 employees)
  - (•) Large (250 or more)

Transparency register number

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

* Country of origin

Please add your country of origin, or that of your organisation.

This list does not represent the official position of the European institutions with regard to the legal status or policy of the entities mentioned. It is a harmonisation of often divergent lists and practices.

- Afghanistan
- Åland Islands
- Albania
- Algeria
- American Samoa
- Andorra
- Angola
- Anguilla
- Antarctica
- Antigua and Barbuda
- Argentina
- Armenia
- Aruba
- Australia
- Austria
- Azerbaijan
- Bahamas
- Bahrain
- Bangladesh
- Barbados
- Belarus
- Belgium
- Belize
- Djibouti
- Dominica
- Dominican Republic
- Ecuador
- Egypt
- El Salvador
- Equatorial Guinea
- Eritrea
- Estonia
- Eswatini
- Ethiopia
- Falkland Islands
- Faroe Islands
- Fiji
- Finland
- France
- French Guiana
- French Polynesia
- French Southern and Antarctic Lands
- Gabon
- Georgia
- Germany
- Ghana
- Libya
- Liechtenstein
- Lithuania
- Luxembourg
- Macau
- Madagascar
- Malawi
- Malaysia
- Maldives
- Mali
- Malta
- Marshall Islands
- Martinique
- Mauritania
- Mauritius
- Mayotte
- Mexico
- Micronesia
- Moldova
- Monaco
- Mongolia
- Montenegro
- Montserrat
- Saint Martin
- Saint Pierre and Miquelon
- Saint Vincent and the Grenadines
- Samoa
- San Marino
- São Tomé and Príncipe
- Saudi Arabia
- Senegal
- Serbia
- Seychelles
- Sierra Leone
- Singapore
- Sint Maarten
- Slovakia
- Slovenia
- Solomon Islands
- Somalia
- South Africa
- South Georgia and the South Sandwich Islands
- South Korea
- South Sudan
- Spain
- Sri Lanka

- Benin
- Bermuda
- Bhutan
- Bolivia
- Bonaire Saint Eustatius and Saba
- Bosnia and Herzegovina
- Botswana
- Bouvet Island
- Brazil
- British Indian Ocean Territory
- British Virgin Islands
- Brunei
- Bulgaria
- Burkina Faso
- Burundi
- Cambodia
- Cameroon
- Canada
- Cape Verde
- Cayman Islands
- Central African Republic
- Chad
- Chile
- China
- Gibraltar
- Greece
- Greenland
- Grenada
- Guadeloupe
- Guam
- Guatemala
- Guernsey
- Guinea
- Guinea-Bissau
- Guyana
- Haiti
- Heard Island and McDonald Islands
- Honduras
- Hong Kong
- Hungary
- Iceland
- India
- Indonesia
- Iran
- Iraq
- Ireland
- Isle of Man
- Israel
- Morocco
- Mozambique
- Myanmar/Burma
- Namibia
- Nauru
- Nepal
- Netherlands
- New Caledonia
- New Zealand
- Nicaragua
- Niger
- Nigeria
- Niue
- Norfolk Island
- Northern Mariana Islands
- North Korea
- North Macedonia
- Norway
- Oman
- Pakistan
- Palau
- Palestine
- Panama
- Sudan
- Suriname
- Svalbard and Jan Mayen
- Sweden
- Switzerland
- Syria
- Taiwan
- Tajikistan
- Tanzania
- Thailand
- The Gambia
- Timor-Leste
- Togo
- Tokelau
- Tonga
- Trinidad and Tobago
- Tunisia
- Türkiye
- Turkmenistan
- Turks and Caicos Islands
- Tuvalu
- Uganda
- Ukraine

- Papua New Guinea
- United Arab Emirates
- Christmas Island
- Italy
- Paraguay
- United Kingdom
- Clipperton
- Jamaica
- Peru
- United States
- Cocos (Keeling) Islands
- Japan
- Philippines
- United States Minor Outlying Islands
- Colombia
- Jersey
- Pitcairn Islands
- Uruguay
- Comoros
- Jordan
- Poland
- US Virgin Islands
- Congo
- Kazakhstan
- Portugal
- Uzbekistan
- Cook Islands
- Kenya
- Puerto Rico
- Vanuatu
- Costa Rica
- Kiribati
- Qatar
- Vatican City
- Côte d'Ivoire
- Kosovo
- Réunion
- Venezuela
- Croatia
- Kuwait
- Romania
- Vietnam
- Cuba
- Kyrgyzstan
- Russia
- Wallis and Futuna
- Curaçao
- Laos
- Rwanda
- Western Sahara
- Cyprus
- Latvia
- Saint Barthélemy
- Yemen
- Czechia
- Lebanon
- Saint Helena Ascension and Tristan da Cunha
- Zambia
- Democratic Republic of the Congo
- Lesotho
- Saint Kitts and Nevis
- Zimbabwe
- Denmark
- Liberia
- Saint Lucia

* Is your organization headquartered in the EU?

- (•) Yes
- ( ) No
- ( ) Other (e.g. multiple organizations)

* Is your parent company headquartered in the EU?

- ( ) Yes
- (•) No

* Scope

-

International

- ○ Local
- ◉ National
- ○ Regional

* Level of governance

- ○ Parliament
- ◉ Authority
- ○ Agency

* **Availability for a follow-up conversation** - We may wish to contact you for clarification or further discussion if your submission prompts additional interest.

Do you agree to be contacted by the Commission for clarification or discussion further to your submission?

- ◉ Yes
- ○ No

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, 'business association, 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* **Contribution publication privacy settings**

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

- ◉ **Anonymous**
  Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.
- ○ **Public**
  Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the

organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.

☑ I agree with the personal data protection provisions

Section 2: Questions for specific target groups

The EU's digital competitiveness in AI and cloud computing is significantly hindered by the gap between the computing resources available in the EU and the needs to satisfy the growing demand for AI-driven services and applications. Current projections indicate that the EU needs to triple its capacity of AI-optimised data and computing infrastructures designed to accommodate data processing and storage needs across the AI value chain (training, inference, fine-tuning). Your response to this section of the survey will help the Commission to assess the scale of this problem as well as to qualitatively analyse its drivers.

2.5 Questions of Public Administrations

* **On behalf of what type of public administration are you answering?**
  - ○ Local
  - ○ Regional
  - ◉ National/Federal
  - ○ European

2.5.1 Current situation

* **Does your public administration currently use cloud computing and AI services?**
  - ◉ Yes
  - ○ No
  - ○ I don't know

* **What types of cloud services do you use?**
  - ☑ Infrastructure as a Service - IaaS (e.g. virtual machines, storage, infrastructure)
  - ☑ Platform as a Service - PaaS
  - ☑ Software as a Service - SaaS
  - ☐ Other
  - ☐ I don't know

* **Do you store data on the cloud?**

- (●) Yes
- ( ) No, only on-premises
- ( ) I don't know

*** What type of data do you store in the cloud?**

- [ ] 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
- [x] Other

* Please specify

1000 character(s) maximum

Information not readily available

*** How do you store this data on the cloud?**

- ( ) All encrypted
- ( ) All non-encrypted
- (●) It depends on the data classification and sensitivity
- ( ) I do not know

*** Please specify the data classification and sensitivity**

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.

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)	○	○	○	○	◉	○
* Cloud provider is headquartered in a third country that poses specific cyber-security threats to the Union	○	○	○	○	◉	○
* 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	○	○	○	○	◉	○
* Other	○	○	○	○	○	◉

* **Which cloud deployment model(s) does your public administration rely on?**

- [x] Government private cloud
- [x] Public cloud
- [x] Hybrid cloud
- [x] Other
- [ ] I don’t know

* Please specify

1000 character(s) maximum

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

* **Are any of your procured providers subject to non-EU jurisdictions including laws with extraterritorial effect (e.g. US or Chinese providers)?**

- ◉ Yes
- ○ No
- ○

I don't know

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)	○	○	○	○	◉	○
* Price	○	○	○	◉	○	○
* Made in the EU	○	○	◉	○	○	○
* Provenance of the provider	○	○	○	◉	○	○
* Integration with other services from the same provider (e. g. software tools)	○	○	◉	○	○	○
* Integration with other services from other providers	○	○	◉	○	○	○
* Interoperability with other providers	○	○	○	○	◉	○
* Integrated offerings (bundle)	○	○	◉	○	○	○
* Sustainability	○	○	○	◉	○	○
* Latency	○	○	◉	○	○	○
* Reliability	○	○	○	◉	○	○
* Scalability	○	○	○	◉	○	○
* Other	○	○	○	○	○	◉

* **Is the software developed in your public administrations released as open source software?**

- ○ Yes
- ◉ No
- ○ I don't know

* **Is there an established public repository where the code can be accessed and contributed to?**

- ◉ Yes
- ○

No

I don't know

* **Is there a community governance mechanism put in place for the code released as open source?**

Yes

No

I don't know

2.5.2 Specific needs and challenges

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	○	○	○	◉	○	○
* Cost efficiency	○	○	◉	○	○	○
* Risk of unlawful access to data from actors subject to non-EU legislation with extraterritorial reach	○	○	○	○	◉	○
* Security mechanisms in place	○	○	○	○	◉	○
* Data protection measures	○	○	○	○	◉	○
* Availability / uptime	○	○	○	◉	○	○
* Performance	○	○	○	◉	○	○
* Integration with other services from the same provider, for instance, software tools	○	○	◉	○	○	○
* Integration with other services from other providers	○	○	◉	○	○	○
* Interoperability with other providers	○	○	○	○	◉	○
* Integrated offering (bundle)	○	◉	○	○	○	○
* Made in Europe	○	○	○	◉	○	○
* Environmental sustainability	○	○	○	◉	○	○
* Protection from cybersecurity risks posed by certain countries	○	○	○	○	◉	○
* Other	○	○	○	○	○	◉

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	○	○	◉	○	○	○
* Security risks	○	○	○	◉	○	○
* Vendor lock in	○	○	○	◉	○	○
* Limited technical expertise	○	○	○	○	◉	○
* Limited or lack of interoperability	○	○	○	◉	○	○
* Regulatory, including public procurement requirements	○	○	○	◉	○	○
* Other	○	○	○	○	○	◉

* **Are there any gaps in the current offerings of cloud computing providers that impact your operations?**

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.

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	○	○	◉	○	○	○
* EU-wide uniform guidance on how to procure	○	○	◉	○	○	○
* Mechanisms to allow federation of cloud services across public administrations within and across Member States	○	○	○	○	◉	○
*						

Standards, open specifications and mechanisms to ensure interoperability of cloud solutions	○	○	○	◉	○	○
* Cybersecurity guidelines	○	○	○	◉	○	○
* Technical support, training and capacity building support	○	○	◉	○	○	○
* Other	○	○	○	○	◉	○

* Please specify

4000 character(s) maximum

- Considering public administrations as a strategic use case for certain critical cloud technologies, in order to attract innovation and investment opportunities for this specific and sensitive use of cloud.

- 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.

* **Does your administration release the code procured for the delivery of digital services as open source?**

- ○ Always
- ◉ In some cases
- ○ Never
- ○ I don't know
- ○ Not applicable

* **What is preventing you from this?**

- ☐ Licenses
- ☐ Cybersecurity vulnerabilities
- ☐ Maintenance
- ☐ Sustainability
- ☐

Accountability

☑ Other

* Please specify

1000 character(s) maximum

information not readily available

* **Are there any specific policy measures you would recommend to improve public administrations' access to and use of cloud services?**

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.

*** Are there any specific policy measures you would recommend for the provision of the security of cloud services for public administrations?**

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.

Please include any additional information you would like to share

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

3. EU Policies

Faced with the current gap in the EU's cloud and AI computing capacity, preliminary policy levers and possible areas of action have been identified to drive the development and deployment of the required computing resources and to stimulate their uptake in line with the EU's rules and broader policy objectives. Your response to this section of the consultation will help the Commission to design the most impactful and efficient policy options as well as identify possible missing elements.

3.1 Computing Capacities

This section collects input on the prioritisation of the activities in order to foster different types of computation facilities in the EU, while taking environmental aspects into consideration.

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).

Facilitation of investment

Policy action	1	2	3	4	5	Not applicable / I don't know

* Increasing public investment in private-public infrastructures	○	◉	○	○	○	○
* Creating public-private partnerships for large-scale data centres	○	◉	○	○	○	○
* Incentives for building computing infrastructure in underserved regions	○	◉	○	○	○	○
* Other	○	○	○	○	◉	○

* Please specify

- 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

-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)

-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

-Facilitate SME acces to cloud and AI infrastructure.

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	◉	○	○	○	○	○
* Reduce the amount of time needed to obtain the different permits and environmental authorisations	○	○	◉	○	○	○
* Create expedited approval mechanisms and clear conditions for critical / strategic projects	◉	○	○	○	○	○
* Other	○	○	○	○	○	◉

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	◉	○	○	○	○	○
* Unified guidelines at EU level	○	○	○	◉	○	○
* Other	○	○	◉	○	○	○

* Please specify

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.

Environmental aspects

Policy action	1	2	3	4	5	Not applicable / I don't know
* Clear environmental compliance requirements	○	○	○	○	◉	○
* Addressing energy availability for data centres	○	○	○	○	◉	○
* Addressing land availability for data centres	○	◉	○	○	○	○
* Other	○	○	○	◉	○	○

* Please specify

Clear requirements on additional sustainability efforts such as capturing heat from data centers.

Energy efficiency

Policy action	1	2	3	4	5	Not applicable / I don't know
* Tax incentives for using sustainable technologies	○	○	○	◉	○	○
* Funding for research and development of energy-efficient technologies.	○	○	○	◉	○	○
* Standardised energy efficiency benchmarks	○	○	○	○	◉	○
* Investments in the development of more efficient software to manage and monitor the energy efficiency and metrics of the data centre	○	○	○	◉	○	○

* Other	○	○	○	○	○	◉

Cross-cutting issues

Policy action	1	2	3	4	5	Not applicable / I don't know
* Supporting an open source software ecosystem	○	○	○	◉	○	○
* Collaborative programmes for R&D and innovation	○	○	○	○	◉	○
* Other	○	○	○	○	◉	○

* Please specify

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.

* **At EU policy level, is it appropriate to distinguish between capacity for training, for fine-tuning, and for inference of AI models and solutions?**

- ◉ Yes
- ○ No
- ○ I don't know

3.2 Public Sector actions

The following set of questions aim at gathering information mainly on the procurement rules of public administrations, and on policy actions to address the challenges faced by the public sector on procuring cloud services.

* **Which EU policy actions would best address the current issues faced by public administrations when procuring cloud and AI services?** (multiple options possible)

- ☑ Guidelines with standard criteria to procure cloud services
- ☑ Guidelines with standard award criteria
- ☑ Standardized tender vocabulary and requirements
- ☐ I don't know
- ☑ Other

* Please specify

1000 character(s) maximum

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.

* **Which EU policy actions would address the issues currently faced by public administrations as regards cloud and AI services?** (multiple options 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
- [x] Marketplace of cloud services, AI services, and other software applications for the Public sector.
- [x] Other
- [ ] I don't know

* Please specify

4000 character(s) maximum

-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.

3.3. Open source in the public sector

The following set of questions are intended to gain input to help address policy options on the release of code developed with public money as open-source code.

* **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)

- [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 setting 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
- [x] Other
- [ ] I don't know

* Other, please specify

4000 character(s) maximum

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.

3.4 Cross – cutting topics

The following questions are intended to provide the Commission with your input on cross-cutting topics such as market practices, security and research.

* **What EU policy actions would address bundling?** Bundling is a commercial strategy where several software packages are sold together for distributon, deployment or use.

- [ ] 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
- [x] Other

* Other, please specify

4000 character(s) maximum

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

* **What EU policy actions would best 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?**

- [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.
- [x] Develop criteria to narrowly identify highly critical use cases for cloud and AI services
- [x] 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
- [ ] I don't know

* The EU pursues and has concluded with third countries agreements that facilitate trusted cross-border data flows and prohibit unjustified data localisation restrictions (including with Japan, Korea, Singapore and the UK). **How important is it in your view that the EU promotes such partnerships with like-minded countries?**

- (•) Very important
- ( ) Somewhat important
- ( ) Neutral
- ( ) Not very important
- ( ) Not important at all

In order to meet the future demand for AI services and applications while catering for the EU's environmental policy objectives and technological autonomy, the EU needs to advance its research and innovation in the area of sustainable and resource-efficient AI computing continuum technologies (IoT, Telco, Edge, the cloud and HPC). Your response to this section of the survey will complement a targeted consultation addressing stakeholders involved in research and innovation projects in these fields and will help the Commission to identify priority fields for future support.

If you are a researcher, are there any specific research priorities that you would like to recommend on:

Data centre components (e.g. highly efficient chips, graphene battery walls)?

4000 character(s) maximum

Optimal data centre operation and use of resources (e.g. AI solutions, optimisation of computing architecture and virtualisation, improved adaptation to user demand)?

4000 character(s) maximum

Cooling innovations (e.g. direct on-chip, liquid & immersive)?

4000 character(s) maximum

Integration of data centres into energy systems?

4000 character(s) maximum

Advanced pilot lines to demonstrate the green data centres of the future?

4000 character(s) maximum

Any other ideas?

4000 character(s) maximum

Please upload your file(s), if you have any additional information

Only files of the type pdf,txt,doc,docx,odt,rtf are allowed

Contact