ESF22-10

Minister Ivan Bartoš
Chair, EU Transport, Telecommunications and Energy Council
Deputy Prime Minister for Digitisation and
Minister of Regional Development
Office of the Government of the Czech Republic
nábřeží Edvarda Beneše 4
118 01, Prague 1 - Czech Republic

Brussels, 1st December 2022

Subject : **ESF call on the draft EU Cybersecurity Certification Scheme for Cloud Services (EUCS)**

Dear Minister Bartoš,

The European Services Forum (ESF) is the European private sector organisation that represents the interests of the European services industries in international trade and investment negotiations. It comprises major European service businesses and European service sector federations covering service sectors including (but not limited to) financial services, telecommunications and IT services, maritime transport, postal and express delivery services, business and professional services, construction, distribution, and audio-visual services. All those services are, in a way or another, provided digitally, and the services sectors are both important cloud service providers (Telecom, IT & Computer services) or customers (bank, insurance, business and management consulting services, telecom, etc).

We are writing to you about the draft Certification Scheme on Cloud Services (EUCS) led by ENISA pursuant to Article 48.2 of the EU Cybersecurity Act ("EUCSA"). We indeed welcome the EU's ambition to harmonise EU-wide standards and improve cybersecurity, but the EUCS must be voluntary, technology neutral, risk-based and focused on concrete security outcome.

We therefore wanted to call your attention on:

- **The de facto mandatory nature of the EUCS**: We understand that ENISA certification is to be implemented on a voluntary basis, like any other one. But first, it is likely that all cloud service providers who want to be active on this segment of business will apply for certification on level 'high', for them to be eligible to supply their services to the governments and the targeted services sectors. Second, we note that in parallel the soon-to-be formally adopted "Network and Information Security" (NIS) Directive allows the EU Commission, via delegated acts, to create *de facto* mandatory certification requirements and further fragmentation instead of "standardization" by introducing a right for Member States to use national certification schemes. ESF is against any attempt to make any certification schemes or any standards mandatory, and we would like to call the attention of the Council on that related matter. We understand that the Council has to take position after the European Parliament vote on that legislation last 10th November.

- **The attempts to introduce "sovereignty requirements" into the EUCS**, namely conditions for cloud service providers who want to qualify for the certificate (under the highest assurance level(s) of the scheme), including a main establishment rule that a company's Headquarter must be in an EU member state and not be owned or controlled by a non-EU entity (so-called "immunity protections"), as well as the requirement for the maintenance, operations and data to be located within the EU, effectively prohibiting international data transfers. These requirements do not seem to allow non-EU headquartered cloud service providers to qualify, potentially preventing such companies in the future to provide cloud services in sectors requiring the highest level of cybersecurity – mandated through legislation – such as Public Sector, Financial services and banking, Energy, Healthcare.

All experts agree that the proposed "sovereignty requirements" will appear to be difficult to implement, and therefore will inevitably lead to higher costs for the cloud service providers. Many EU cloud service providers might not be able to meet these requirements and hence might not be able to compete in the European market for cloud service providers.

Furthermore, should non-EU cloud service providers not be allowed any more to serve their EU customers, a very large number of European businesses will not have any suitable alternatives at least in the short to middle term, which will cause serious disruption in their daily operations and on a broader perspective, in the on-going digital transformation in the European Union's economy. It is also unclear how global operations from European businesses could be maintained in the long term if the data needs to be localised in Europe.

So, these "sovereignty requirements" will have the exact counter-effect by either preventing companies and governments to procure the most efficient, secured, innovative, and competing cloud services; or by having to use different cloud services in the various region of the world where they operate; or by obliging European companies to procure cloud services inside the EU with possibly lower standards and hence increasing the cybersecurity risks. The European service industries are all in favour of strengthening the EU cybersecurity, but we believe that the Europe's data governance should be non-discriminatory and take a transatlantic mindset. We share the views that EU digital regulation should not hamper the EU single market, the transatlantic trade or the development of SME's or start-ups, and should not breach the EU international commitments, leading to a loss of its credibility internationally.

The **European Services Forum is mainly active in the field of trade policy**. We aim at ensuring that any possible EU internal measures should not breach obligations in existing trade-agreements or hamper on-going of future trade negotiations (bilateral, plurilateral or multilateral) and the relationships between the EU and its trading partners.

Digital trade barriers are on the rise all around the world, as the OECD Digital Services Trade Restrictiveness Index (DSTRI) shows. In the G20 alone, more than 1700 legal acts regarding the digital economy were adopted since 2020, without any recognizable alignment and coordination. These barriers are slowing the digital transformation, increasing the cost of the green transition of the world economy. The European Union trade negotiators do their utmost efforts in all on-going trade negotiations to persuade non-EU countries not to introduce localisation barriers in their own domestic regulation. This is the case in bilateral trade negotiations as well as in the ongoing WTO E-Commerce negotiations taking place in Geneva,

Should the EUCS certification scheme be adopted as currently suggested, we are particularly concerned that it will be inconsistent with:

- **the EU position in the ongoing WTO E-Commerce** where the EU is proposing that "**cross-border data flows shall not be restricted by**: (a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements **that are certified or approved in the territory of the Member**; (b) **requiring the localization of data in the Member's territory for storage or processing**; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localization requirements in the Member's territory". Clearly, the suggested EUCS certification scheme will effectively be a data localisation requirement and an outright market access barrier. The EU will then seriously lose credibility in asking other countries not to do so.

- **The rules on the preparation of technical regulations in the Agreement on Technical Barriers to Trade (the "TBT Agreement") and the WTO plurilateral Agreement on Government Procurement**, to which the EU is a Party. Indeed, the EU negotiators are active in ensuring that technical barriers to trade should be avoided. But this new proposal using certification processes will be a counter example. Technical barriers to trade are more and more introduced in the digital sphere all over the world, and often imposing new protectionist regulations to products, as well as to embedded services.

- **The EU's WTO commitments** and commitments made under **many exiting Free Trade Agreements.** The EU has committed to national treatment and most-favoured nations obligations, notably in its **GATS schedule of commitments**[1] and FTAs services schedules of commitments notably under "computer related services". ESF would argue that the current proposal risks to violate these commitments and hence possibly be duly subject to dispute settlements requests.

[1] See EU GATS Schedule in "Computer and Related Services" (page 31&32). See GATS Annex on Financial services as well. See Schedules of Services Commitments in EU FTAs on DG Trade website (e.g. EU-UK TCA, EU-Japan EPA, EU-Singapore FTA, etc.).

- The EU's principle of free movement of data (personal and non-personal) within the EU and outward, which is enshrined in EU law itself (including the Free Flow of Data Regulation and the General Data Protection Regulation - GDPR). Hence, localisation requirements or other highly restrictive requirements run counter to the EU's proper regulation.

- The EU efforts in supporting the rules-based trading system and an equitable reform of the WTO, with the risks of undermining its own credibility in negotiating international treaties.

Taking all the above into consideration, we encourage the Council to:

- Hold the further development of the mentioned "sovereignty requirements" in the cloud security scheme (EUCS) until a proper political and legal assessment is undertaken and stakeholders have been consulted in line with the EU's transparency and better regulation principles. We are concerned that already now, because of the proliferation of these measures outside the public and democratic sphere, trade in services and relationships with the EU's trading partners have suffered. At the very least, such matter should be discussed at the EU Council level, and we join many EU member states representatives on this subject and call upon the Czech Presidency to ensure that such an item is discussed at the next meeting of the Telecom ministers at the Transport, Telecommunications and Energy Council, scheduled to take place on 6th December 2022 in Brussels. Regarding the suggestions to integrate those requirements in the cloud certification scheme, a thorough political discussion on all consequences with all stakeholders must take place. At technical level, a transparent process of creating EUCS is a must through public consultations amongst all parties affected and involve cloud cybersecurity experts.

- Use multilateral and bilateral dialogues - like the EU-US Trade and Technology Council (TTC) framework- that can also be an effective avenue to discuss and reach a political agreement to tackle issues like "immunity requirements" or other conflicts of law; also considering European Commission adequacy decisions - like the incoming EU-US Data Privacy Framework - which will tackle surveillance concerns through an agreed mechanism. This will restore certainty for enterprises and ensure free flows of data.

By essence, certification must comply with international trade commitments and principles, such as non-discrimination, the least trade-restrictive policy option and proportionality. It should refrain from including political requirements and be limited to technical specifications. How data is protected is more important than where it is stored. Hence, there are other means in reaching the highest level of cybersecurity than introducing protectionist measures, and we call all the stakeholders concerns to reconsider their recommendations.

In any event, before taking any action, a proper legal and economic impact assessment of the requirements musts be conducted and it should include a study on all possible economic effects, involving due consultations of relevant private sector stakeholders, both providers and consumers of cloud services.

We are grateful for your attention and for taking these comments into consideration. ESF and its members remain at your disposal for any further information on that matter.

Yours sincerely,

Annette Meijer
ESF Chair

Cc: Minister of European Affairs Mikuláš Bek, Czech Presidency
Executive Vice President of the European Commission, Valdis Dombrovskis
European Commissioner for Internal Market, Thierry Breton,
President Charles Michel, Council of the European Union
General Secretariat of the Council
Council's Working Party on Telecommunications and Information Society
Council's Trade Policy Committee

List of members supporting the above position

- Amfori
- Apple
- Architects' Council of Europe –ACE
- British Telecom Plc
- BDO
- Bureau International des Producteurs et Intermédiaires d'Assurances – BIPAR
- BUSINESSEUROPE
- BUSINESSEUROPE WTO Working Group
- BSA The Software Alliance – BSA
- Danish Shipping
- Deutsche Post DHL
- DI – Confederation of Danish Industries
- Digital Europe
- EK - Confederation of Finnish Industries
- EuroCommerce
- European Community Shipowners' Associations – ECSA
- European Express Association – EEA
- Fédération de l'Industrie Européenne de la Construction – FIEC
- FratiniVergano European Lawyers
- General Council of the Bar of England & Wales
- Google
- Huawei Europe
- IBM Europe, Middle East & Africa
- Insurance Europe
- Irish Business and Employers' Confederation - IBEC
- Law Society of England & Wales
- Microsoft Corporation Europe
- Prudential Plc.
- Svenskt Näringsliv (Confederation of Swedish Enterprise)
- TechUK
- Telenor Group
- TheCityUK
- UPS
- Vodafone
- Zurich Insurance