Centrum für Europäische Politik
FREIBURG | BERLIN

cepInput

No. 8 | 2025 25 April 2025

EU Cloud Certification at an Impasse

(Escape) routes leading to a resilient cloud policy in the EU

Philipp Eckhardt and Anja Hoffmann

The establishment of an EU scheme for certifying the cybersecurity of cloud services (EUCS) has been under discussion for years. However, debates about the inclusion of so-called sovereignty requirements in an EUCS are delaying an agreement. Such requirements are intended to strengthen the cybersecurity of cloud services, but they could make it more difficult for cloud users in the EU to use cloud services based in third countries. This cepInput outlines ways out of the deadlocked discussion surrounding the EUCS and presents proposals for a resilient EU cloud policy. Time is of the essence because cloud infrastructure is hugely important in terms of digital and security policy.

- If adequately designed, an EUCS could revitalise the market for cyber-secure cloud services and strengthen the confidence of potential users in such services. The promotion of cyber-secure cloud services that simultaneously support the EU's digital sovereignty also seems appropriate from a geopolitical and security policy perspective. However, from an economic perspective, an EUCS that includes sovereignty requirements would not only have advantages but also some disadvantages and would also be problematic from a legal perspective.
- The Commission should specifically adapt the EU Cybersecurity Act (CSA), the Network and Information Security Directive (NIS-2) and the EU rules on public procurement in order to establish a resilient EU cloud policy. Until the adapted legislation comes into force, the Commission should – as a transitional solution – develop and adopt guidelines for "sovereign" cloud services and for transparency regarding the characteristics of such cloud services.

Table of Contents

1 Introduction[1]

In his report on the future of European competitiveness published in September 2024, Mario Draghi, former Prime Minister of Italy and President of the European Central Bank (ECB), made a sobering statement: "The EU cloud services market is also largely lost to US-based players" and "the EU's competitive disadvantage will likely widen in cloud computing". According to the Synergy Research Group, alone the three cloud service providers known as "hyperscalers" – Amazon Web Services, Microsoft Azure and Google Cloud – already cover 65% of the EU market. In the second quarter of 2024, their combined shares of the global market amounted to 67% (32%, 23% and 12%). At the same time, the market share of EU providers is steadily declining in a constantly growing market that is expected to reach a volume of EUR 200 billion (2022: approx. EUR 87 billion).[2,3,4] According to analyses, more than half of corporate IT expenditure will be spent on cloud investments by 2025, more than on traditional IT. [5,6]

Back in 2020, the EU Commission pointed out in its EU data strategy[7] that it considers cloud infrastructure and services to be essential for the digital transformation of the EU economy and warned that "the EU must reduce its technological dependence on such strategic infrastructure [...]". In particular, it criticised that this dependency makes the EU "vulnerable to external threats", that a third country could gain unwanted access to data of EU citizens and companies via a third country provider operating in the EU, and that legitimate concerns arise regarding the application or applicability of foreign legislation to EU companies, citizens and authorities. It also noted that there were uncertainties as to whether cloud service providers from third countries were actually complying with EU rules and standards.[8] The Body of European Regulators for Electronic Communications (BEREC) also emphasised in a report from April 2024 that the lack of equivalent European solutions poses significant risks for the digital transformation of industrial ecosystems in the EU, for example with regard to possible disruption of cloud services from third countries, existing lock-in effects and unlawful access to data.[9,10]

The huge dependence on cloud service providers from third countries and, in particular, on the US hyperscalers has therefore led to calls in recent years for the EU to strengthen its "digital sovereignty"

---

1 This cepInput is an updated version of a cepInput published in German in December 2024 (s. here).

2 EU Commission (2024a), The future of European competitiveness, Part B: In-depth analysis and recommendations, Report by Mario Draghi, September 2024, p. 77.

3 Synergy Research Group (2024), Cloud Market Growth Stays Strong in Q2, While Amazon, Google and Oracle Nudge Higher, RENO, NV, 1 August 2024, see here.

4 The Body of European Regulators for Electronic Communications (BEREC), for example, points to significant barriers to market entry, as the provision of cloud services requires considerable investment in infrastructure, IT resources and specialised personnel. The sector is also characterised by "significant sunk costs, economies of scale and scope and ecosystem effects" [BEREC (2024), BEREC Report on Cloud and Edge Computing Services, BoR (24) 52, 7 March 2024]. Mario Draghi's report also points to the comparatively high property and energy costs in the EU as a barrier to providers based in the EU [EU Commission (2024a)].

5 Gartner (2022), Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025, 9 February 2022.

6 GEREK (2024).

7 EU Commission (2020a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020) 66, A European Data Strategy, 19 February 2020.

8 EU Commission (2020), p. 10.

9 EU Commission (2022), SWD(2022) 41, Commission Staff Working Document, EU strategic dependencies and capacities: second stage of in-depth reviews, 22 February 2022.

10 In its "Budapest Declaration", the European Council called on the Commission to present proposals by June 2025 to "strengthen the EU's technological capabilities" and to exploit the opportunities of the data economy "while ensuring privacy and security" [European Council (2024), Budapest Declaration on the New Deal for European Competitiveness, 8 November 2024].

in the area of cloud computing. In 2023, if not before, this discussion also found its way into the debate surrounding the establishment of a European Cybersecurity Certification Scheme for Cloud Services (EUCS) when requirements were to be integrated into this EUCS that would have potentially restricted the use of cloud services from third countries.

This cep**Input** will start by taking a closer look at the controversial debate surrounding the EUCS before subsequently developing ideas for a future resilient EU cloud policy. Section 2 begins by explaining the key requirements of the EU Cybersecurity Act (CSA)[11]. Section 3 then takes a closer look at the EU scheme for certifying the cybersecurity of cloud services (EUCS), which is currently under development, and in particular at the discussion surrounding the inclusion of so-called sovereignty requirements in such a scheme. It also analyses what such a cloud certification scheme can and cannot achieve as well as the extent to which sovereignty requirements are appropriate or necessary from a (political) economic perspective and whether it seems legally justifiable to enshrine them in a cloud certification scheme. Finally, against the backdrop of the launch of the new EU Commission, Chapter 4 outlines possible ways out of the muddled situation and presents proposals for a future resilient cloud policy. The study will then be rounded off by way of the conclusion (Chapter 5).

[11] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

2 Requirements of the EU Cybersecurity Act

2.1 Context

In April 2019, the EU Cybersecurity Act [CSA, (EU) 2019/881[12]] came into force. The Regulation defines the objectives, tasks and organisational aspects of the EU Agency for Cybersecurity (ENISA) and also creates a framework for certifying the cybersecurity of ICT products, services and processes at EU level.

This certification framework is designed to ensure that certified ICT products, services and processes sold in the EU comply with EU cybersecurity standards. To this end, ENISA is developing so-called European cybersecurity certification schemes, which define standardised EU-wide security requirements and assessment criteria for certain ICT products, services and processes. These schemes are then adopted by the Commission in the form of implementing acts. Manufacturers and providers can then have their products, services or processes evaluated according to the corresponding scheme or, if necessary, evaluate them themselves. If they meet the security requirements set out in the respective scheme, they can be issued with a European cybersecurity certificate or an EU declaration of conformity, which certifies compliance with the requirements and is recognised in all EU Member States. European cybersecurity certification schemes are intended to help harmonise cybersecurity procedures in the EU.[13]

The EU framework for cybersecurity certification is intended to pursue several objectives in this respect. It will

- ensure an "adequate level of cybersecurity",[14]
- prevent a "fragmentation of the internal market" with regard to cybersecurity certification,[15]
- increase trust in ICT products, services and processes[16] and
- help to avoid the emergence or parallel existence of costly, diverse, conflicting or overlapping national cybersecurity certification schemes, thereby reducing costs for organisations.[17]

2.2 Development of European schemes for cybersecurity certification

EU schemes for cybersecurity certification are developed by ENISA[18] and adopted by the Commission via implementing acts.[19] As a rule, the Commission mandates[20] ENISA to develop a scheme, that the Commission has already announced in the so-called "Union rolling work programme for cybersecurity certification"[21], for certain[22] ICT products, services or processes listed in the programme.[23] This work programme is updated by the EU Commission at least once every three years.[24] In justified cases, the

12 Regulation (EU) 2019/881.
13 Recital 95 Regulation (EU) 2019/881.
14 Art. 1 (1) (b) Regulation (EU) 2019/881.
15 Art. 1 (1) (b) Regulation (EU) 2019/881.
16 Recital 65 and 69 Regulation (EU) 2019/881.
17 Recital 69 Regulation (EU) 2019/881.
18 Art. 49 (1) Regulation (EU) 2019/881.
19 Art. 49 (7) Regulation (EU) 2019/881.
20 In doing so, the Commission "should" also "evaluate the positive and negative impact of its request on the specific market in question especially its impact on SMEs, on innovation, on barriers to entry to that market and on costs to end users" [Recital 84 Regulation (EU) 2019/881].
21 Art. 47 Regulation (EU) 2019/881.
22 Art. 47 (2) Regulation (EU) 2019/881.
23 Art. 48 (1) Regulation (EU) 2019/881.
24 Art. 47 (5) sentence 2 Regulation (EU) 2019/881.

Commission – and also the "European Group for Cybersecurity Certification (EGCZ)"[25] – can ask ENISA to develop a scheme that was not included in the work programme.[26]

In principle, all ICT products, services and processes that are subject to an assessment during cybersecurity certification must fulfil the security requirements specified in the respective scheme. The requirements are intended to "the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle"[27]. Therefore, each scheme must realise several security objectives. Among other things, it must protect "stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process" and ensure that "authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer".[28] In addition, one or more assurance levels – basic, substantial and/or high – must be specified for each scheme. Each level must be commensurate with the level of risk associated with the use of a particular ICT product, service or process, taking into account the probability and impact of a potential security incident.[29] For each assurance level included in the scheme, the corresponding security requirements and evaluation criteria – which differ depending on the level – are defined in the respective scheme.[30] Providers seeking a certificate for the highest assurance level must then fulfil higher requirements or undergo a stricter assessment than if they want to apply for a certificate for a lower level.

Any scheme developed by ENISA will only become applicable after it has been adopted by the Commission by means of an implementing act. The so-called "examination procedure" is used to adopt the legal act.[31] This procedure allows Member States to prevent the adoption of a new scheme under certain conditions.[32] The Commission must submit the draft implementing act to a review committee made up of representatives of the Member States.[33] In addition, the EU Cybersecurity Regulation stipulates that the Commission may not adopt a European scheme before the review committee has issued an opinion.[34] If the committee rejects the draft scheme, the Commission must amend the draft or appeal to the appeal committee.[35] If the latter also rejects the application, the Commission may not adopt the legal act nor therefore the scheme.[36]

2.3 Voluntary or mandatory cybersecurity certification?

The use of European cybersecurity certification is basically "voluntary". However, this only applies as long as EU law or the law of the Member States does not stipulate otherwise.[37] The EU expressly

[25] The "European Cybersecurity Certification Group" is composed of representatives of the national cybersecurity accreditation authorities or representatives of other relevant national authorities [Art. 62 Regulation (EU) 2019/881].
[26] Art. 48 (2) and Recital 84 Regulation (EU) 2019/881.
[27] Art. 46 (2) Regulation (EU) 2019/881.
[28] Art. 51 Regulation (EU) 2019/881.
[29] Art. 52 (1) Regulation (EU) 2019/881.
[30] Art. 52 (3) Regulation (EU) 2019/881.
[31] Art. 49 (7) in conjunction with Art. 66 (2) Regulation (EU) 2019/881, which refers to Art. 5 (4) (b) of the EU Comitology Regulation (EU) No. 182/2011 (Regulation (EU) 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers).
[32] Cf. Art. 3 (3) Regulation (EU) 182/2011.
[33] Art. 3 (3) Regulation (EU) 182/2011.
[34] Art. 66 (2) Regulation (EU) 2019/881, which refers to Art. 5 (4) (b) Regulation (EU) No. 182/2011.
[35] Art. 5 (3) Regulation (EU) 182/2011.
[36] Art. 6 (3) sentence 3 Regulation (EU) 182/2011.
[37] Art. 56 (2) Regulation (EU) 2019/881.

reserves the right to make EU certification mandatory under EU law for certain ICT products, services or -processes, in the future.[38] Specifically, Directive (EU) 2022/2555 (NIS 2 Directive)[39] gives the Commission the power, under certain conditions, to require, by means of a delegated act, essential[40] and important[41] entities to use only certain certified ICT products and services or to obtain an EU cybersecurity certificate.[42] Member States may also oblige essential and important entities only to use products with an EU cybersecurity certificate (see also Box 1).[43] They can also take European cybersecurity certification into account, particularly in public tenders and the awarding of public contracts.[44]

Box 1: Use of EU cybersecurity certification schemes by essential/important entities

According to Directive (EU) 2022/2555 (NIS 2 Directive)[45], **Member States** "may" require "essential" and "important" entities to use certain ICT products and services – which may include cloud services – that[46]
- are developed by the organisation itself or procured from third parties and
- have been certified under an EU cybersecurity certification scheme.

The draft of the German "NIS-2 Implementation and Cybersecurity Strengthening Act" of July 2024, for example, provides that the "Federal Ministry of the Interior and Home Affairs" will be able to prescribe by statutory order that (particularly) important entities may only use certain ICT products and ICT services certified according to an EU cybersecurity certification scheme. This applies if[47]
- the products or services are "relevant" for the provision of the entity's services, and
- the "nature and extent of the entity's exposure to risk" make the mandatory use of certified products or services "necessary".[48]

Furthermore, the **Commission** may determine for individual categories of essential and important entities[49]that these[50]
- may only use certain certified ICT products and services, or
- must obtain an EU cybersecurity certificate.

2.4 Ineffectiveness of conflicting national schemes for cybersecurity certification

In addition, the EU Cybersecurity Act (CSA) stipulates that any existing national cybersecurity certification schemes will become ineffective if they are overlaid by an EU scheme. This is the case if or as soon as an applicable EU scheme covers ICT products, services and processes that are also the subject of a

38 Art. 56 (3) and Recital 92 Regulation(EU) 2019/881.
39 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 ("NIS 2 Directive").
40 "Essential" entities include, for example, companies in the energy, transport, finance and healthcare sectors as well as public administrations [Art. 3 NIS 2 Directive].
41 "Important" entities include, for example, companies in the postal and food sectors as well as companies in the manufacturing industry [Art. 3 NIS 2 Directive].
42 Art. 24 (2) NIS-2 Directive.
43 Art. 24 (1) NIS-2 Directive.
44 Recital 91 Regulation (EU) 2019/881.
45 Art. 24 (1) sentence 1 NIS-2 Directive.
46 Art. 24 (1) NIS-2 Directive.
47 German Federal Ministry of the Interior and Home Affairs (2024), NIS-2 Implementation and Cybersecurity Strengthening Act, 22 July 2024, see Section 30 (6) and Section 56 (3).
48 If the Commission has already prescribed delegated acts for the mandatory use of such schemes, these acts take precedence over a provision issued by statutory order. The Federal Ministry of the Interior and Home Affairs must also coordinate with other departments before issuing a statutory order. It must also check whether a scheme exists at all and whether sufficient certified ICT products or ICT services are available on the market.
49 Such a determination is made through the adoption of delegated acts. Such a decree is only possible if an "inadequate level of cybersecurity" has been established [Art. 24 (2) NIS-2 Directive].
50 Art. 24 (2) NIS-2 Directive.

national scheme and is intended to avoid fragmentation of the internal market.[51] The Commission will determine the date on which existing national schemes become ineffective in its decision on adopting the EU scheme. Covered ICT products may then no longer be certified nationally; however, national certificates that have already been issued remain valid until the end of their period of validity.[52] Member States cannot introduce any new schemes that conflict with an EU scheme. In contrast, national schemes for ICT products, services and processes that do not fall under such an EU scheme remain in place.[53] However, Member States may exceptionally introduce or maintain conflicting national schemes if they consider this necessary for "reasons of national cybersecurity".[54]

2.5 Further principles for EU cybersecurity certification schemes

Finally, the following two additional principles apply in particular to cybersecurity certification schemes: Firstly, the EU cybersecurity certification schemes "should" be "non-discriminatory"[55]. Secondly, they "should" be "established in a uniform manner in all Member States".[56] The EU-wide uniform introduction is intended to prevent "certification shopping" – i.e. the targeted application for certification in the Member State with the lowest level of requirements.[57]

3 The EU Cybersecurity Certification Scheme for Cloud Services (EUCS)

3.1 General Information

On 9 December 2019, the Commission commissioned ENISA to develop an EU cybersecurity certification scheme for cloud services ["European Cybersecurity Certification Scheme for Cloud Services (EUCS)"].[58] The Commission's main reason for the mandate was to strengthen and tighten cybersecurity standards for cloud services in the EU internal market. There is currently a patchwork of cybersecurity standards for cloud services in the EU. In Germany, for example, the so-called C5 criteria catalogue (Cloud Computing Compliance Criteria Catalogue) of the German Federal Office for Information Security (BSI) defines minimum requirements for secure cloud computing.[59] The Commission sees the different national schemes in the EU Member States as a challenge for the certification of cloud services and regards the EUCS as a means of overcoming this problem.[60] The EUCS aims to harmonise the cybersecurity certification of cloud services in the EU in line with international standards and industry best practices and to create a transition from current national certification schemes to a single EU-wide cybersecurity certification scheme for cloud services. At the same time, the Commission considers an EUCS to be necessary in order to "stimulate cloud uptake in Europe" because cloud services represent a fundamental technology for development in many technological areas.[61]

---

51 Recital 94 Regulation (EU) 2019/881.
52 Art. 57 (3) Regulation (EU) 2019/881.
53 Art. 57 (1) sentence 2 Regulation (EU) 2019/881.
54 Recital 94 Regulation (EU) 2019/881.
55 Recital 69 Regulation (EU) 2019/881.
56 Recital 70 Regulation (EU) 2019/881.
57 Recital 70 Regulation (EU) 2019/881.
58 EU Commission (2019), Towards a more secure and trusted cloud in Europe, see here.
59 Federal Office for Information Security, Criteria Catalogue C5, see here. Cloud services can be certified by auditors according to "BSI C5" on the basis of the strict criteria of this test standard and then receive a so-called C5 certificate after successful testing, see FAQ C5 of the BSI.
60 EU Commission (2021), EU Cloud Certification Scheme, 9 June 2021, see here.
61 ENISA (2020a), EUCS – Cloud Services Scheme, December 2020, p. 10, see here.

In December 2020, ENISA presented a first draft of the EUCS and put it out for consultation.[62] The EUCS draft provides for the establishment of a "horizontal" scheme for a wide range of cloud services – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), etc.[63] The EUCS defines basic security requirements for cloud services that are based on existing national systems and international standards. It is designed as a voluntary scheme, covers three assurance levels – basic, substantial and high – and is intended to grant certification for three years, which can be renewed.[64] The EUCS is intended to act as a "technical tool" that provides potential customers of cloud services with information and thus enables them to make informed decisions.[65] It aims to ensure cybersecurity throughout the entire cloud supply chain and to provide a basis on which to set up sectoral schemes.[66]

Since presenting its first draft for the EUCS, ENISA has already revised it several times. Nevertheless, the Commission has still not finally adopted the EUCS by means of an implementing act – after more than four years. This is due in particular to a long-standing discussion about the possible inclusion of so-called "sovereignty requirements" in the scheme. This discussion, that regained a fresh momentum after the publication of a draft report on “European technological sovereignty and digital infrastructure” in late February 2025[67], will be dealt with in more detail below.

3.2 Discussion on sovereignty requirements in a future EUCS

The term "sovereignty requirements" refers to requirements that are intended to ensure or increase the sovereignty of the EU. This refers in particular to requirements designed to prevent third countries from accessing certain information, such as the obligation to store data only in the EU or to subject contracts exclusively to EU law. The debate on the introduction of sovereignty requirements is illustrated below with a selection of different versions of the EUCS.

First version of the EUCS draft of December 2020: In ENISA's first draft of an EUCS in December 2020, sovereignty requirements played at best a subordinate role. In fact, ENISA explicitly emphasised that the planned EUCS scheme should not set requirements that restrict the geographical location for the storage or processing of the data or restrict the applicable law. However, it demanded that cloud service providers must be transparent about the geographical location of the data and the applicable law. For example, cloud service providers were to provide information about the locations of all system components on which their customers' data is stored or processed. The first draft of the EUCS envisaged a total of three assurance levels for certification – low (basic), substantial and high. A certification for assurance level "high" should be suitable for all cloud services that are intended to fulfil special security requirements – beyond the medium level – for "business-critical data and systems" and are able to "minimise the risk of state-of-the-art cyberattacks by actors with extensive capabilities and resources".[68] At this highest security level, cloud service providers should also have to document which

---

62 ENISA (2020b), Cloud Certification Scheme: Building Trusted Cloud Services Across Europe, ENISA launches a public consultation on a new draft candidate cybersecurity certification scheme in a move to enhance trust in cloud services across Europe, Press Release, 22 December, 2020, see here.

63 ENISA (2020a), p. 11.

64 ENISA (2020b).

65 ENISA (2020a), p. 11.

66 ENISA (2020b); also ENISA (2021), Consultation on the draft EUCS, see here.

67 European Parliament (2025), Draft Report on European technological sovereignty and digital infrastructure, Committee on Industry, Research and Energy (ITRE), Rapporteur: Sarah Knafo, 25. February 2025.

68 ENISA (2020a), p. 20; see also Art. 52 (7) Regulation (EU) 2019/881.

support services are provided from which locations. This information should then be published together with the certificate once certification has been completed.[69]

Version of the EUCS draft of May 2023: However, this approach did not stop there. In a revised draft in May 2023, ENISA proposed for the first time specific sovereignty requirements that go beyond mere transparency requirements[70]. Among other things, ENISA introduced a number of new requirements designed to ensure that the assessed cloud service was independent from non-EU legislation and, in particular, requirements relating to the location of data storage and processing, the location of employees authorised to access data and the effective control of the cloud service provider [71] At the same time, ENISA proposed splitting the assurance level "high" into two separate "evaluation levels" (EL) – CS-EL3 and CS-EL4. While evaluation level CS-EL3, like the assurance level "high" in the original draft, would be suitable for all cloud services that are intended to fulfil special security requirements for business-critical data and systems that go beyond the second assurance level "substantial", evaluation level CS-EL4 is aimed at the "most sensitive" cloud services. This includes all cloud services that process particularly sensitive personal or non-personal data, the violation of which "is likely to result in a breach of public order, public safety, human life or health or the protection of intellectual property".[72]

The sovereignty requirements were defined in more detail in a new Annex J and divided into four groups. The requirements of group one (PUA-01) were to ensure the primacy of EU law. The requirements of group two (PUA-02) contained specifications for the locations at which certified cloud services are operated and maintained and customer data is stored and processed. The requirements of group three (PUA-03) were intended to control access by employees and business partners outside the EU. Finally, the requirements of group four (PUA-04) would ensure that third countries could not gain or exercise any effective control over the certified cloud service providers.

Some of these new requirements in group one were intended to apply to all assurance levels. For example, already in order to obtain a certification at the lower and medium assurance levels (now referred to as evaluation levels CS-EL 1 and CS-EL 2), cloud service providers would have to ensure that their contracts for cloud services were governed by the law of an EU Member State, were only to be interpreted in accordance with this law and that only courts or adjudicative bodies in the EU Member States had jurisdiction to settle contractual disputes. However, the strictest sovereignty requirements would apply to the assurance level "high". The EUCS draft of 2023 therefore provided inter alia for the following additional requirements for evaluation levels CS-EL 3 and CS-EL 4 and the restrictive requirements for level CS-EL 4 went well beyond level CS-EL 3:[73]

1. Primacy of EU law and independence from non-EU law:

The cloud service providers would

[69] ENISA (2020a), p. 11 and 151 (DOC-03 Data Processing and Storage) and 215 (F 6.2).
[70] ENISA (2023), EUCS – Cloud Services Scheme, V.1.0.319, May 2023.
[71] ENISA (2023), p. 6.
[72] ENISA (2023), p. 26, 28, 31 and 32. According to ENISA, this particularly sensitive data includes, firstly, legally protected secrets such as data on government consultations, national security and defence, foreign policy or court proceedings. Secondly, evaluation level CS-EL 4 would also apply "to the protection of privacy", medical secrecy and business secrets, including information on production methods, economics and finance, as well as business and industrial strategies. Thirdly, level CS-EL 4 covered all data required for the fulfilment of essential state tasks such as safeguarding national security, maintaining public order and protecting human life and health. In contrast, evaluation level CS-EL 3 is "intended for use cases in which independence from non-EU law is an important factor", albeit to an extent that can vary from provider to provider depending on the exact use case and the legal structure of the cloud provider (p. 28).
[73] ENISA (2023), p. 301– 306.

- to ensure independence from non-EU law, be additionally required to include, as from evaluation level CS-EL 3, certain risks in their global risk assessment related to the possible extraterritorial application of conflicting non-EU law; this includes in particular the risk of foreign authorities gaining access via this third-country law to commercially sensitive business information and trade secrets, for the processing of which no prior consent has been obtained from the owner of the information or the legal persons named in it (requirement PUA-01.2H),
- have to provide their customers with information on (residual) risks for their own risk assessment on request (requirement PUA-01.3H),
- contractually undertake to consider only investigation requests made on the basis of EU or Member State law (requirement PUA-01.5H), and
- go beyond this mere contractual obligation and implement technical and organisational measures to ensure that they do not actually comply with any investigation requests that have not been made on the basis of EU law or the law of an EU Member State; although this latter requirement only applied at the highest evaluation level CS-EL 4 (requirement: PUA-01.6H).

2. Operation of the cloud service in the EU:

- For certification under evaluation level CS-EL 3, cloud service providers would not be obliged to provide and manage their services, including support, only from locations in the EU or to store and process all customer data exclusively at locations in the EU. However, they should maintain transparency about these locations and must contractually offer their customers at least one option in which all specified locations are in the EU (requirement PUA 02.1H in conjunction with DOC-02.1H).[74]
- In contrast, the requirements for certification under evaluation level CS-EL 4 were not merely limited to a contractual customer option for data storage and processing in the EU but generally obliged the cloud service provider to fully localise and process data within the EU. Thus, all system components on which the cloud service provider or its sub-service providers stored and processed customer data had to be located exclusively in the EU. In addition, cloud services had to be managed and monitored only from locations within the EU and support services only provided from such locations. At most, only individual, precisely specified support activities and, under exceptional circumstances regulated in the contract, certain other activities, would be allowed to be provided from a third country by way of exception. Here too, however, the provider would also have to offer an option guaranteeing complete data localisation in the EU without the aforesaid exceptions (requirement PUA-02.1H).

3. Control over access by employees and business partners in third countries

Cloud service providers would

- also have to ensure, as from evaluation level CS-EL 3, that only those employees who are either located in the EU or who are monitored by a pre-screened, EU-resident employee, are granted access to the cloud customer's data (requirement: PUA-03.1H), and furthermore
- be obliged to check all service providers that provide support for functional components of the cloud service, in advance, or have them monitored by a certified employee located in the EU who could intervene in real time if necessary and prohibit further access (requirement PUA-03.2H). All maintenance activities should be logged, checked and archived (requirement PUA-03.3H).

[74] ENISA (2023), p. 306.

4. EU headquarters and corporate governance requirements of the cloud service provider

- Finally, the most sensitive cloud services and therefore those to be certified according to evaluation level CS-EL 4 would have to fulfil additional requirements – going beyond level CS-EL 3 – in order to ensure "effective control of the cloud service provider"[75] . The draft stipulated that both the registered head office and the global headquarters of these providers had to be located in the EU (requirement PUA-04.1H). ENISA also wanted to stipulate that companies from third countries must not hold effective control[76] of the cloud service provider – neither directly nor indirectly and neither alone nor together with other companies (requirement PUA-04.2H). This would "mitigate the risk of non-EU interfering powers undermining EU regulation, norms and values".[77]

The most important additional sovereignty requirements of the EUCS draft of May 2023 can therefore be summarised as follows:

- Contracts for the provision of certified cloud services must be governed by the law of a Member State and stipulate that only courts or adjudicative bodies in the EU have jurisdiction over disputes relating to the contracts.
- In order to obtain certification at evaluation level CS-EL 3, the cloud service provider may only access its customers' data where control is exercised by employees who have undergone special checks and are based in the EU. It must also carry out a risk assessment in connection with the extraterritorial application of non-EU laws. In contrast, the draft did not in principle restrict the geographical location of the data or its processing at this level to the EU but merely required the provider to be transparent about its locations and jurisdiction.[78]
- In order to obtain certification at the strictest evaluation level CS-EL 4, the provider must also have its registered headquarters and global head office in the EU and must not be subject to effective control by non-EU companies. In addition, all locations where customer data is stored or otherwise processed or from which support is provided or the cloud service is managed or maintained must be located within the EU. As compared to the first draft version, although the EUCS was designed as a "technical tool", ENISA consequently proposed restrictions on the applicable law, the geographical location of data processing and the registered office of the cloud service provider in order to obtain certification at the CS-EL 4 evaluation level.[79]

Version of the EUCS draft of March 2024: After lengthy discussions and interventions, including by the governments of individual Member States, such sovereignty requirements are no longer included in the latest version of the EUCS of March 2024.[80] In addition to the lower and middle levels, there is still the assurance level "high"; within this, however, no distinction is now made between evaluation levels CS-EL 3 and CS-EL 4. As before, the level "high" will apply to all cloud services designed to protect "mission-critical data and systems" – such as sensitive and confidential data from businesses and governments. This assurance level is also considered suitable for cloud services that are designed to meet sector-specific requirements with regard to global business activities. ENISA is explicitly thinking of the financial sector here.[81]

---

75 ENISA (2023), p. 25 and 26.
76 With regard to the term "control", ENISA referred to the EC Merger Regulation (EC) No 139/2004.
77 ENISA (2023), p. 305.
78 ENISA (2023), p. 15.
79 ENISA (2023), p. 15.
80 ENISA (2024), EUCS – Cloud Services Scheme, V1.0.413, March 2024.
81 ENISA (2024), p. 24.

The restrictive sovereignty requirements described above, on the other hand, are to be explicitly omitted; Annex J has been removed from the draft. Only the "requirements of the primacy of EU law" in the governance of contracts are to remain in place (requirement: A.5, CO-05.1B), according to which cloud service providers must operate "primarily" within EU law and the law of the Member States. As in the EUCS draft of 2023[82], contracts between cloud service providers seeking certification of their cloud service and users of their cloud service at each of the three assurance levels must be governed by the law of an EU Member State, must be interpreted only in accordance with that law and must give exclusive jurisdiction to courts or adjudicative bodies in EU Member States to settle contractual disputes, and not to courts, tribunals or arbitration bodies from third countries.[83]

As in the original version, cloud service providers must ultimately maintain transparency about the jurisdiction and all locations where data is processed, stored and backed up, regardless of the assurance level.[84]

However, this does not mean that the introduction of strict sovereignty requirements into the EUCS is off the table. In fact, there have since been discussions behind the scenes about reintroducing such criteria into the draft, although this has recently been described as unlikely.[85] ENISA has still not published a final draft.

3.3 What can an EU cybersecurity certification scheme for cloud services achieve?

The establishment of an EU cybersecurity certification scheme for cloud services makes sense in principle because such a scheme can counter existing information asymmetries. The extent to which users of cloud services – whether consumers, companies or government bodies – are able to assess the cybersecurity of the cloud services they do not (yet) use is often limited. This lack of information reduces their willingness to pay for the supposedly more secure cloud services. As a result, cloud service providers also have fewer incentives to invest in the cybersecurity of their services. As a result, the markets for cloud services frequently exhibit characteristics of "markets for lemons".

The planned EUCS can make an important contribution to tackling this problem. If properly designed, it could revitalise the market for cyber-secure cloud services as well as strengthening the confidence of potential users in such services. The EUCS could therefore be a vehicle for strengthening both trust in the use of cloud services per se and the associated transfer of data to "trustworthy" third parties. A recently published survey shows that trust in IT security, data protection and compliance play the most important role (99%) when selecting cloud providers. The fear of unauthorised access to sensitive data for 64% of respondents and the loss of data for 52% are also relevant obstacles to the implementation of cloud projects.[86] However, strengthening user trust can only be achieved if the scheme is considered credible and trustworthy by users. In addition, the following must always be considered: Certifying the cybersecurity of cloud services tends to go hand in hand with an increase in the cost of services. This could slow down the development of a flourishing market for cyber-secure cloud services. And although an EUCS is an important element of European cybersecurity policy, it is not a panacea because it does not address two problems in particular. Firstly, cloud service users are still incentivised not to

82 ENISA (2023), Annex J, requirement PUA-01.1B.
83 ENISA (2024), p. 100.
84 ENISA (2024), p. 145.
85 Gkritsi, E. (2024), Sovereignty requirements for cloud providers unlikely to make it to Commission's proposal for implementing act, 26. June 2024, see here.
86 Bitkom (2024), Cloud Report 2024, Welche Rolle spielt die Cloud für die deutsche Wirtschaft?, 3.July 2024.

attach the necessary economic importance to cyber risks when selecting such a service. Even an EUCS will not prevent users from regularly avoiding the full costs of cybersecurity incidents as they can outsource damage to other players. They do not factor these negative consequences of an incident into their decision-making (non-internalisation of external effects). Secondly, an EUCS cannot prevent free-rider behaviour because third parties often benefit from the fact that citizens, companies or the state use a cyber-secure cloud service without having to make any contribution of their own to those paying citizens, companies or states for this "additional profit". The buyers or users of the cyber-secure cloud service are not rewarded for generating such a positive external effect. However, this in turn reduces their willingness to invest in cyber-secure services, as they rely on the fact that third parties will bear the additional costs associated with more secure cloud services. Addressing these two issues – non-internalisation of externalities and free-rider behaviour – requires other specific policy measures. One of these measures was, for example, the adoption of the EU Cyber Resilience Act (see cep**PolicyBrief**)[87].

It is appropriate that the EUCS is primarily designed as a voluntary certification scheme. If the acquisition of a certificate were mandatory for cloud service providers in every case, this could act as an unnecessary and expensive barrier to market entry and slow down innovation. Firstly, an obligation for cybersecurity certification only seems justifiable in highly sensitive areas of application – which ones these are is primarily a (societal) political decision.[88] Secondly, it seems justifiable in cases where the use of an "insecure" cloud service by a private, commercial or government user causes or could cause major cybersecurity risks for third parties.

3.4 Are sovereignty requirements appropriate?

3.4.1 Purpose and potential benefits of the requirements

The implementation of sovereignty requirements in a future EUCS, which has now been announced, has three dimensions: an industrial policy dimension, a security and geopolitical dimension and a dimension focussing on the single market. These three dimensions must be considered both separately and together.

In the industrial policy context, sovereignty requirements are intended to increase the barriers to market entry for providers of cloud services from third countries or make their further participation in the market more difficult and reduce dependence on these providers. In this sense, the sovereignty requirements thus serve as an instrument of market foreclosure. On the other hand, they are intended as a measure that will make it easier for cloud service providers from the EU to enter the market or to maintain or even expand their existing footprint in the market. In this sense, the requirements therefore serve as an instrument for market liberalisation.[89] In its communication on "Shaping Europe's digital future" in February 2019, the Commission emphasised the importance of ensuring the "integrity and resilience" of data infrastructures, networks and communications in the EU and called for the

[87] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Regulation).

[88] Such a decision was essentially taken in the context of the definition of essential and important entities as part of the revision of the Directive on measures to ensure a high common level of security of network and information systems in the EU (so-called NIS 2 Directive (EU) 2016/1148) (see new Directive (EU) 2022/2555 on measures for a high common level of cybersecurity in the EU).

[89] Blancato, F. G. (2024) also sees the efforts to safeguard data sovereignty – which is one element of digital sovereignty – as an "integral part of an industrial policy toolkit" with which the EU wants to protect local cloud providers from foreign competition [Blancato, F. G. (2024), The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem, Policy & Internet, 16(1), 12-32].

"right conditions" to be established in the EU so that Europe can "develop and deploy its own key capabilities" and reduce "our dependency on other parts of the globe for the most crucial technologies". This is crucial for Europe's "digital sovereignty"[90].[91] In its mandate to ENISA to develop the EUCS, the Commission also emphasised that this should not only be an instrument to strengthen the cybersecurity of cloud services in the internal market, but also one to "promote the use of cloud services in Europe".[92] Sovereignty requirements are thus also a means of strengthening the EU's competitiveness in the technology sector[93] and ensuring that EU companies can continue to gain a foothold where technological sovereignty is deemed necessary, and thus that Europe cannot dispense with the development of its domestic technology sector.[94] In addition, standardised EU-wide sovereignty requirements may enable economies of scale, as cloud service providers will not have to be certified according to different national requirements. This can also potentially reduce costs for users of certified cloud services. Sovereignty requirements could also be justified with the argument that they might weaken existing monopolistic or oligopolistic tendencies in the EU markets for cloud services and thus strengthen resilience[95] – as the three US companies Amazon, Microsoft and Google currently cover over 60% of the EU cloud market.[96]

At the same time, sovereignty requirements have a momentum arising from security policy and geopolitics, which is also reflected in the term "digital sovereignty". There is great public interest in providing European companies and authorities with "access to secure, sustainable and interoperable cloud infrastructures and services" and in being able to maintain this access.[97] Ultimately, the establishment of "minimum viable clouds" – i.e. "trustworthy EU cloud environments with sufficient and secure capabilities" – is a question of safeguarding national security.[98] This applies in particular to information of high national importance, where maintaining data security in the cloud is of immense importance and a strategic priority for Member States.[99] Sovereignty requirements aim to ensure certain "immunity from non-EU law"[100]. They are also intended to strengthen information security and help maintain sovereignty over data – especially data and information that is considered particularly sensitive. Accordingly, ENISA emphasises the need to give special protection to data whose violation may

[90] Kreutzer et al. (2022) define "digital sovereignty" as "the ability to realise one's own goals in a self-determined manner without being restricted or even hindered in self-determined action due to insufficient or non-existent control over key digital technologies and skills". The concept of digital sovereignty must be distinguished from both self-sufficiency and heteronomy, as sovereignty can often only be achieved through networking with other actors" [Kreutzer, S. et al. (2022), Wie Europa seine digitale Souveränität wiederherstellen kann].

[91] EU Commission (2020b), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Shaping Europe's digital future, COM(2020) 67, 19 February 2020.

[92] ENISA (2020a), p. 10.

[93] Kenneth Propp, Peter Swire and Josh Fox (2023), Oceans Apart: The EU and US Cybersecurity Certification Standards for Cloud Services, 11 July 2023.

[94] EU Commission (2024a).

[95] See also A. Wolf (2024), **cepInput** No. 14, Resilience Auctions for Net-Zero Technologies, An Effective Market-based Measure to Shield the Green Transition?, 24 September 2024, p. 6. Following this line of argument, sovereignty requirements would be obsolete as soon as the monopoly or oligopoly positions were overcome [A. Wolf (2024), p. 6].

[96] Synergy Research Group (2024).

[97] See here.

[98] Alexandre Gomes and Maaike Okano-Heijmans (2024), Too late to act? Europe's quest for cloud sovereignty, Clingendael, Netherlands Institute of International Relations, March 2024. The authors emphasise that the diversification of European solutions is not a luxury but a necessity.

[99] Raman, S. (2023), Two Visions of Digital Sovereignty. Joint PIJIP/TLS Research Paper Series, American University Washington College of Law.

[100] "Immunity from non-EU law" ultimately means that cloud providers who process or store the data of cloud users in the EU should be subject to EU law alone. The law of a third country should not apply to them.

jeopardise public order, public security, human life, health or the protection of intellectual property.[101] In addition, sovereignty requirements can also be seen as a kind of precaution against a targeted denial of access to cloud services used from third countries, or against the unplanned failure or cancellation of these services, especially against the backdrop of growing geopolitical uncertainties and risks.[102] If cloud services as a critical digital technology come from just one or a few countries and there is a "high concentration of global supply" in this regard, this also means a high level of dependence on the industrial and trade policy of these countries, which could then use this geostrategic position of power as a diplomatic leverage.[103,104] Furthermore, sovereignty requirements should emphasise that the EU also wants to be able to implement and enforce its own rules in the future ("regulatory sovereignty") and be able to evade any requests from security and law enforcement authorities in third countries, for example.[105]

A third purpose that uniform EU-wide sovereignty requirements promise to fulfil is to avoid the fragmentation of such requirements in the internal market. France serves as a prime example here. For example, the French government established a "cloud at the centre" doctrine that imposes sovereignty requirements on public institutions in France when using cloud services.[106] The country also introduced a mandatory cybersecurity certification scheme under the title "SecNumCloud". Certifications under the scheme are awarded by the National Agency for Cybersecurity (ANSSI). The scheme also contains provisions on protection against non-EU law.[107,108] It is generally regarded as the blueprint for the sovereignty requirements now provided for under the EUCS.[109] If other Member States were to follow this example, the result would be a proliferation of different provisions in the EU or they would perpetuate themselves. Thus, on the one hand, this would encourage potential distortions of competition. This applies in particular to companies that are based in different Member States but compete with each other. If these companies were subject to different strict requirements when selecting authorised cloud services, it would lead to competitive advantages or competitive disadvantages for the companies concerned. In addition, companies in the individual Member States may have to fulfil different and conflicting requirements, which would result in higher costs and additional work, particularly for cloud service providers that are active in several Member States. Harmonised sovereignty requirements in the EUCS would not only avoid such distortions of competition, but uniform requirements would also make it easier to apply the law and create legal consistency.

3.4.2 Fears and potential risks of sovereignty requirements

The central objective of any EU cybersecurity certification framework is to ensure an "appropriate level of cybersecurity".[110] The same applies to the notional EUCS. In particular, at the highest level of

[101] ENISA (2023).
[102] Raman, S. (2023).
[103] A. Wolf (2024), p. 6.
[104] The announcement by US Vice President-designate JD Vance that the USA could refuse to support NATO if the "X" platform is over-regulated in the EU shows that such or similar steps are not entirely unrealistic (see also here).
[105] Kenneth Propp (2022), European Cybersecurity Regulation Takes a Sovereign Turn, European Law Blog, 12 September 2022.
[106] The doctrine was adopted in July 2021 and updated at the end of May 2023 (see here).
[107] SecNumCloud, for example, stipulates that the cloud service provider must be based in an EU Member State and imposes restrictions on ownership.
[108] Premier ministre (2022), Agence nationale de la sécurité des systèmes d'information, Prestataires de services d'informatique en nuage (SecNumCloud), référentiel d'exigences, Version 3.2, 8. March 2022.
[109] Christakis, T. (2024), The "Zero Risk" Fallacy: International Data Transfers, Foreign Governments' Access to Data and the Need for a Risk-Based Approach.
[110] Art. 1 Regulation (EU) 2019/881.

assurance, it must be designed to "intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources".[111] It is now sometimes emphasised that sovereignty requirements do not increase cybersecurity but may tend to impair it.[112] For example, access to potentially more mature and cyber-secure (non-EU) cloud solutions and services would be restricted for cloud users. Localisation specifications would also require more data centres, which could be compromised. There would need to be an increase in (qualified) personnel to maintain the various cloud service locations, which may not always be available in sufficient numbers. More locations and employees also increase the potential attack surface for attackers. Access to and exchange of information about (potential) cyber threats would also be more difficult if the relevant information could not be shared across borders. In addition, sovereignty requirements could lead to a reduced distribution of (sensitive) information and thus encourage the emergence of concentration risks. Overall, they would also contribute to complicating the management of cyber risks.[113,114,115] And last but not least, the market compartmentalisation associated with sovereignty requirements could lead to cloud users having to rely on one or a few compliant providers and thus being driven into a (new) dependency, which would not be a sensible strategy from a security perspective.[116]

In addition to the risk of cybersecurity being weakened by sovereignty requirements, there are also other concerns. They could be perceived as a protectionist step and encourage third countries to introduce counter or retaliatory measures that make it difficult or impossible for EU cloud providers to access the markets of third countries. This would be particularly damaging for globally active suppliers who are active in these markets or want to be present there. International trade would be disrupted. On the other hand, sovereignty requirements limit the market supply, restrict the freedom of choice for cloud service consumers and thus weaken competition. This may increase the prices for users of the services and thus their costs. Even apart from the capabilities of third-country cloud providers in terms of defence against cyber threats and combating cybersecurity incidents, which are at risk of being lost due to sovereignty requirements, these requirements also mean a potential loss of access to innovations and features of these cloud service providers – which are crucial for our own competitive positioning. Last but not least, data localisation requirements could also contribute to (sustainability-related) inefficiencies, as the choice of location for data and data centres is restricted. These could possibly no longer be positioned where energy is greenest, energy costs are lowest and the availability of water resources is greatest.[117]

Finally, Christakis, T. (2024) points out that cloud providers who promise to fulfil the sovereignty requirements – and thus immunity from non-EU law – would probably not be able to make this promise in relation to the US in every case if they themselves also operate in the US. This is because they could still be affected by US law and may be required to respond to enquiries from US authorities.[118]

---

[111] ENISA (2023), EUCS – Cloud Services Scheme, V.1.0.319, May 2023, p. 25.

[112] Blancato, F. G. (2024) points out that policy efforts on the territoriality of data ultimately contradict the concept of data itself. If data is processed or stored in the cloud, this does not usually take place at a specific location or in a specific jurisdiction.

[113] Raman, S. (2023).

[114] Swire, P., & Kennedy-Mayo, D. (2022), The Effects of Data Localization on Cybersecurity. Georgia Tech Scheller College of Business Research Paper, 4030905.

[115] Bauer, M., & Lamprecht, P. (2023), The economic impacts of the proposed EUCS exclusionary requirements estimates for EU member states (No. 04/2023), ECIPE Occasional Paper.

[116] Alexandre Gomes and Maaike Okano-Heijmans (2024).

[117] Raman, S. (2023); Bauer, M., & Lamprecht, P. (2023); Alexandre Gomes and Maaike Okano-Heijmans (2024).

[118] Christakis, T. (2024).

According to this assessment, the requirements for sovereignty would be partially ineffective and therefore ultimately unnecessary.

3.4.3 Are sovereignty requirements in the interests of (potential) cloud users?

The extent to which sovereignty requirements would meet with approval on the user side in view of this mixed situation cannot be clearly determined. The survey cited above shows that trust in IT security, data protection and compliance plays a central role for potential cloud users. However, whether data centres should be located in Germany or the EU, for example, and/or come from a trustworthy country of origin is only of great importance to just under 60% of respondents. At the same time, however, 53% and 96% of survey participants say that they would not consider the USA or China as a location for individual data centres, and for 98% the location of the data centres per se is a relevant factor. And a large number of survey participants also attach great importance to the performance of the cloud services offered (97%).[119] Whether strict sovereignty requirements are actually wanted in practice therefore appears to be an open question at present.

3.5 Legal perspective – lawfulness of sovereignty requirements

3.5.1 Compatibility with the EU Cybersecurity Act (CSA)

Firstly, the question arises as to whether and to what extent the introduction of sovereignty requirements in an EUCS by the EU Commission is covered by the EU Cybersecurity Act (CSA) as the "basic instrument". If this were not the case, the Commission would possibly move outside the scope of its competences provided for by the CSA if it were to adopt an EUCS with sovereignty requirements.

But what framework does the CSA provide? Art. 1 (2) of the CSA firstly clarifies that the competences of the Member States for activities relating to public security, national defence, national security and state action in the area of criminal law remain unaffected. However, this does not generally exclude these areas from the scope of the CSA. However, the narrow area of national security of the Member States is excluded from EU competence as this remains the sole responsibility of each EU Member State in accordance with Art. 4 (2) sentence 3 of the Treaty on European Union (TEU).[120] Since the EU is and was not permitted to take regulatory action in this area, the CSA cannot in any case provide a lawful basis for sovereignty requirements in an EUCS that fall within the area of national security reserved to the Member States. Such provisions in an EUCS would therefore not be lawful.

In most cases, however, sovereignty requirements are unlikely to relate to the narrow area of national security. The European Cybersecurity Certification Framework was created to increase the level of cybersecurity in the EU".[121] "Cybersecurity" means all activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats.[122] A "cyber threat", in turn, is any circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons.[123] Because the CSA cannot set out all the "cybersecurity requirements" of all ICT products, services and processes in detail, the European cybersecurity certification schemes are intended to ensure that the ICT products, services and processes certified according to their specifications comply with specified requirements

[119] Bitkom (2024), Cloud Report 2024, Welche Rolle spielt die Cloud für die deutsche Wirtschaft?, 3 July 2024.
[120] For more information on national security, see section 3.5.2 below.
[121] Art. 46 (1) Regulation (EU) 2019/881.
[122] Art. 2 No. 1 Regulation (EU) 2019/881.
[123] Art. 2 No. 8 Regulation (EU) 2019/881.

aimed at realising the security objectives set out in Art. 51 of the CSA.[124] These security objectives principally involve safeguarding the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, functions or services that are offered by or made accessible via these products, services and processes throughout their life cycle.[125] The schemes must regulate the relevant cybersecurity objectives and specify in detail how these objectives are to be achieved for certain ICT services (in this case cloud services).

It is questionable to what extent the sovereignty requirements contained in the EUCS draft – in particular the location of the registered office, the requirement for data localisation and the requirements for corporate control – can be qualified as "cybersecurity" requirements. It could be argued that these requirements are not purely technical but in fact rather legal in nature. However, the requirements should at least also serve the aforementioned security objectives, as their purpose is to prevent unauthorised access to data and cloud services from third countries. The CSA does not explicitly stipulate which requirements ENISA or the Commission may or may not regulate in detail in a cybersecurity certification scheme for cloud services; most notably, it does not stipulate that the schemes may only regulate technical details. It can be inferred from Art. 52 (3) that the "security requirements" – this includes the "security functionalities" of the services as well as the criteria for the rigour and depth of the evaluation – are to be regulated in the scheme. The CSA does not define what a "security functionality" is. Whether requirements for independence from third-country law constitute a "security functionality" of a cloud service is nevertheless questionable. In addition, the CSA refers in several places to the fact that "technical specifications" and/or standards can or must be referenced in the schemes. It calls for European cybersecurity certification schemes to "be built on what already exists at international and national level and, if necessary, on technical specifications from forums and consortia", learning from current strengths and assessing and correcting weaknesses.[126] Accordingly, it stipulates that each scheme must at least contain, among other things, references to the standards or technical specifications relevant for the assessment.[127] This suggests that the Commission can and should regulate at least primarily technical aspects in the schemes.

It should also be noted that the Commission adopts a scheme like the EUCS drawn up by ENISA in a so-called committee procedure as an implementing act.[128] In the CSA, the EU legislator was and is authorised to delegate to the Commission the power to regulate important details of certification in implementing regulations.[129] However, according to the case law of the European Court of Justice (CJEU), the legislator is obliged to regulate all essential aspects itself.[130] The essential provisions of a subject-matter are to be regulated in the basic legislative act. The adoption of provisions requiring political decisions that fall within the EU legislator's own remit must therefore not be delegated to the Commission.[131] The CJEU only considers provisions that give concrete shape to the fundamental guidelines

[124] See Recital 75 Regulation (EU) 2019/881.
[125] See recital 75 and Art. 51 of Regulation (EU) 2019/881 particularly (a), (b) and (c) thereof.
[126] Recital 71 Regulation (EU) 2019/881. Similarly, Recital 69 provides that the schemes should be non-discriminatory and based on European or international standards, unless these standards are ineffective or inappropriate to fulfil the Union's legitimate objectives in this area.
[127] Art. 54 (1) (c) Regulation (EU) 2019/881.
[128] Art. 49 (7), Art. 66 (2) Regulation (EU) 2019/881.
[129] Eckhardt. P. / Hoffmann, A., Cybersecurity Part 2 – Certification, cep**PolicyBrief** No. 16/2018.
[130] The concept of essential elements is also reflected in the requirement for a legal basis under EU law when restricting fundamental rights, which was codified in Art. 52 (1) of the EU Charter of Fundamental Rights. See section 3.5.5 below for more details.
[131] CJEU, Judgement of 5 September 2012, CaseC-355/10 – EP v. Council, C-176/03, ECLI:EU:C:2012:516, para. 64, 65.

of EU policy as "essential".[132] It is true that Art. 291 of the Treaty on the Functioning of the European Union (TFEU), which regulates implementing acts, does not contain an explicit reference to the fact that the adoption of essential provisions is reserved to the legislator, unlike Art. 290, which regulates the power of the EU Commission to adopt so-called delegated acts. However, this is not necessary, as implementing acts cannot, by their very nature, influence the essential elements of the basic legislative act.[133]

The limits of the Commission's powers must be assessed on the basis of the main objectives of the basic legislative act – in this case the CSA. The Commission may take all measures necessary and appropriate for implementation, provided that they do not infringe the fundamental provisions of the basic legislative act, do not interfere with its essential features and do not alter its scope.[134] Implementing regulations are merely intended to further specify the rules in the basic legislative act in order to ensure its uniform implementation in the Member States.[135]

The proponents of sovereignty requirements want to harmonise these requirements for the entire EU, and the CSA also specifies the basic orientation of the certification itself with the security objectives, elements and effects of the schemes. However, by including restrictive sovereignty requirements that require cloud service providers to localise all data in the EU, have their headquarters in the EU and be immune to third-country law, the Commission would not merely be "specifying" existing technical or legal criteria to strengthen cybersecurity in the EU by means of a filler without any political effect but would also in fact be supplementing essential aspects and thereby adding a new dimension to the EUCS, which is not legally possible in implementing acts.

Which aspects are to be categorised as essential must be assessed objectively. The characteristics and particularities of the relevant subject area must be taken into account.[136] In the area of delegated acts, too, the more political a decision is, the more likely it is to be considered "essential".[137] At the very least, mandatory sovereignty requirements, such as the requirement for mandatory company domicile and company control as well as data localisation to be in the EU, are of fundamental political importance as they can significantly influence the cloud market in the EU and also involve risks affecting trade policy and other areas.[138] They would potentially strengthen European cloud service providers; at the same time, they could make it more difficult for providers from third countries to operate on the European market, especially when it comes to cloud services at the highest assurance level. Opponents of sovereignty requirements also claim that EU authorities and companies could be forced to switch to providers with economically inadequate, less secure or simply more expensive services.[139] In view of the possible complex political implications, at least the decision on the introduction of mandatory sovereignty requirements must be regarded as "essential".

Which path the EU chooses in this respect to protect itself from the influence of third countries is therefore a question of the fundamental direction of EU policy, which is reserved for the EU legislator. This is confirmed not least by the many years of controversial and inconclusive political discussion among Member States about the inclusion of sovereignty requirements in the EUCS draft. During the

[132] CJEU, Judgement of 27 October 1992, Case C-240/90, Germany v. Commission, ECLI:EU:C:1992:408, para. 37.
[133] Schmidt, F., in: von der Groeben,H./Schwarze, J./Hatje, A., AEUV, 7th Edn. 2015, Art. 291, para. 14.
[134] Gellermann, M. , in: Streinz, R., EUV/AEUV, 3rd Edn. 2018, para. 12.
[135] Nettesheim, M., in: Grabitz, E./Hilf, M./Nettesheim, M., AEUV Art. 291 para. 40.
[136] CJEU, Judgement of 5 September 2012, CaseC-355/10 – EP v. Council, C-176/03, ECLI:EU:C:2012:516, para. 67f.
[137] Nettesheim, M., (loc. cit.), Art. 291 para. 41.
[138] See section 3.4.2 above for more details.
[139] Propp (2023), Oceans apart: The EU and US Cybersecurity Certification Standards for Cloud Services, available here.

debate, countries such as the Netherlands have therefore rightly argued that the issue of sovereignty requirements must be dealt with at the European political level.[140] As a result, the mandatory introduction of the sovereignty requirements described above is an essential political decision that cannot be taken by the Commission and ENISA, but only by the legislator.[141] The EU should therefore regulate any sovereignty requirements by law. Firstly, a proper EU legislative procedure would enable a more transparent debate on the rationale and impact of sovereignty requirements, with the involvement of the European Parliament. Secondly, solid impact assessments and market acceptance studies are required in order to make an informed decision on whether – and if so, which – sovereignty requirements should be introduced.

3.5.2 Powers to regulate sovereignty requirements, subsidiarity and proportionality vis-à-vis the Member States

When (re)regulating EU-wide sovereignty and cybersecurity requirements by law, the EU could possibly rely on the competence to harmonise the internal market [Art. 114 TFEU]. As the example of the French SecNumCloud shows, the French government has already introduced a mandatory cybersecurity certification scheme that also includes sovereignty requirements. Harmonised legislation at EU level would prevent fragmentation of the internal market due to different sovereignty requirements in the Member States and thus help to create a functioning internal market for cloud services. However, in order to exclusively regulate specific requirements for cloud services, the EU might principally have to use the legislative competence for the harmonisation of the trade in services under Art. 53 (1) in conjunction with Art. 62 TFEU, which is specific to the fundamental freedoms. However, based on these provisions, the EU could only adopt a directive to coordinate the Member States' legislation on the "taking-up and pursuit" of cloud services in the EU. The EU should check this carefully and duly justify its choice of legal basis.

However, the EU's competences end as soon as the legislation affects the protection of the national security of the Member States. As already explained, protection of national security remains the sole responsibility and competence of the EU Member States in accordance with Art. 4 (2) sentence 3 of the Treaty on the European Union (TEU).[142] Consequently, the EU cannot regulate sovereignty requirements in areas that fall within the national security of Member States, or must exclude these areas from its provisions. As the CJEU ruled in the Schrems II judgement, the aforementioned provision in the TEU exclusively concerns the "Member States"[143] and thus the distribution of competences within Europe – it protects the EU Member States from excessive EU intervention in this important national core competence. In contrast, third parties (e.g. third countries or companies from third countries) cannot invoke this provision.[144]

The term "national security" must be interpreted more narrowly than the term "public security". It only covers disruptions to public safety that are of national importance, i.e. that affect the security of

[140] Opinion of the Netherlands on the non-paper by DE, ES, FR and IT on the EUCS requirements for immunity from non-EU laws (2021), available here.

[141] Thus in general (i.e. not referring to the present case) Ruffert, M., in Calliess, C./Ruffert, M., EUV/AEUV, 6th Edn. 2022, AEUV Art. 290 para. 15.

[142] This is therefore a reservation of competence by the Member States, see Obwexer, W., in: Von der Groeben, H./Schwarze, J./Hatje, A., Europäisches Unionsrecht, 7th Edition 2015, Art. 4 EUV para. 46.

[143] CJEU, C-311/18 (Data Protection Officer/Facebook Ireland Ltd and Maximilian Schrems, Judgment of 16 July 2020, ECLI:EU:C:2020:559, "Schrems II", para. 81.

[144] CJEU, C-311/18 (Data Protection Officer/Facebook Ireland Ltd and Maximilian Schrems, Judgment of 16 July 2020, ECLI:EU:C:2020:559, "Schrems II", para. 81.

the state itself.[145] Which sovereignty requirements for which providers, data and systems fall within the narrow scope of national security must be examined more closely.

However, sovereignty requirements generally go beyond the protection of national security and can also serve broader legitimate objectives. These can range from creating a basis of trust for the wider use of cloud services by strengthening cybersecurity through improved data privacy, to the protection of public security and order in EU Member States. Legislative competence for the internal market is a competence shared between the EU and the Member States.[146] Both the EU and the Member States may in principle regulate sovereignty requirements in order to realise the internal market. However, it is a concurrent competence in the sense that the Member States lose their power to act if and insofar as the Union has exercised its competence.[147]

If and insofar as the EU has not yet taken action to issue an EUCS or regulate sovereignty requirements for cloud services, the Member States may still maintain their own cybersecurity certification schemes at national level. However, as soon as the Union utilises the legislative powers it has been granted, the national legislators in the Member States are subject to a blocking effect.[148] This arises both from Art. 2 (2) sentences 2 and 3 TFEU and specifically from Art. 57 (1)-(3) CSA. According to this provision in the CSA, once the EU has adopted an EUCS, Member States may no longer introduce or maintain competing cybersecurity certification schemes; existing schemes will become ineffective ("cease to produce effects").

If the EU makes use of its competence and regulates sovereignty requirements or an EU-wide EUCS, it must – in addition to the limitation on the exercise of powers in relation to national security – observe the principle of subsidiarity pursuant to Art. 5 (3) and the principle of proportionality pursuant to Art. 5 (4) of the Treaty on European Union (TEU). A high (technical) level of cybersecurity across the EU can generally best be achieved at EU level. However, any EU-wide regulation of cybersecurity and sovereignty requirements for cloud services encroaches on the authority of the Member States to regulate the level of cybersecurity or other security interests in their state, independently and in a self-determined manner. Mandatory EU-wide legislation could lead to a reduction in the level of protection in the Member States. Member States should also be able to make the use of cloud services subject to stricter (national) conditions and sovereignty requirements, or retain these, insofar as the protection of important fundamental national interests such as public security, national defence or public order is concerned – including those that go beyond the narrow area of "national security". However, where existing national schemes overlap with an EUCS adopted by the EU, the Member States would have to adapt their schemes so that they only apply to the regulatory areas reserved for them in accordance with the above-mentioned rules and, in particular, the principle of proportionality.

However, as already mentioned above, when it comes to protecting national security, which remains within their sole competence, Member States may also provide for or maintain (supplementary) sovereignty requirements, possibly with a higher level of protection, which serve to protect national security. In principle, they could also include these requirements in a (supplementary) national scheme for cybersecurity certification. This is also reflected in Recital 94 of the CSA, which recognises that

[145] "State security", see CJEU, Judgement of 29. 1. 2008, Case C-275/06 – promusicae, ECLI:EU:C:2008:54, para. 49 ; see also Schill, S./Krenn, C, in: Grabitz, E./ Hilf, M./Nettesheim, M., Art. 4 EUV para. 42.
[146] Art. 4 (2) (a), Art. 2 (2) of the Treaty on the Functioning of the EU (TFEU).
[147] Art. 2 (2) sentence 2 TFEU; cf. also Nettesheim, M., in: Grabitz, E./Hilf, M./Nettesheim, M., Art. 2 AEUV para. 25.
[148] Nettesheim, M., loc. cit.

Member States may exceptionally adopt or maintain national cybersecurity certification schemes "for national security purposes".

3.5.3 Overlaps and compatibility with the EU Data Act

The "EU Data Act" (see cep**PolicyBrief**)[149], which came into force in December 2023, already contains some requirements that are very similar to some of the sovereignty requirements discussed in connection with the EUCS. Firstly, it obliges providers of data processing services – including cloud and edge services – to take "adequate" respectively "reasonable" technical, organisational and legal measures (such as contractual agreements) to prevent unlawful governmental access by third-country authorities to non-personal data stored in the EU or its transfer to third-country authorities if such access or transfer would create a conflict with EU or national law.[150] Secondly, it provides that judgements and decisions of courts or administrative authorities in third countries, requiring a provider of data processing services to transfer or grant access to non-personal data, may only be recognised or enforced in the EU if this is covered by a legally binding international agreement, such as a mutual legal assistance treaty. This provision corresponds to Art. 48 of the General Data Protection Regulation (GDPR)[151], which regulates the same in the event that a judgement or decision of a third country requires a controller or processor – in this case also the cloud service provider – to transfer or disclose personal data. Both laws prohibit cloud service providers from transferring data out of the EU solely on the basis of unilateral decisions by a third country. They are thus intended to prevent that extraterritorial authorities access data directly from private companies (i.e. the cloud services providers) in violation of international law by circumventing or omitting state channels or without procedural guarantees under the rule of law.[152] However, the Data Act goes even further than the GDPR in that it also sets out rules for providers regarding the granting of access to or transfer of data to third countries in the absence of an international agreement.[153] Thirdly, the Data Act requires providers of data processing services to inform their customers of any data access request from third-country authorities before complying with it, unless the request is for law enforcement purposes and is necessary to carry out effective law enforcement measures.[154] Fourthly, they need to maintain transparency, and their websites must:

- provide information on the jurisdiction to which their ICT infrastructure deployed for data processing is subject; and

[149] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Regulation).

[150] Art. 32 (1) Regulation and Recital 102 (EU) 2023/2854 (EU Data Act). These measures involve the implementation of protective measures by cloud service providers. These safeguards aim to enable EU citizens, public authorities and companies to retain control over their data and maintain EU standards with regard to "security, data protection, privacy and consumer protection". Cloud service providers must seek to prevent unlawful government access from third countries, where reasonable, by "encryption of data, frequent submission to audits, verified adherence to relevant security reassurance certification schemes and by the modification of corporate policies" [Recital 102 Data Act].

[151] The European Data Protection Board (EDPB) published guidelines on Art. 48 GDPR on 3 December 2024. The guidelines 02/2024 are intended to help companies and organisations to decide whether and under what conditions they may lawfully transfer personal data to authorities from third countries if they are requested to do so. In the guidelines, the EDPB also highlights possible legal bases under Art. 6 GDPR and the necessary grounds under Art. 44 et seq. GDPR for such a data transfer. At the same time, all stakeholders and citizens currently have until 27 January 2025 to submit their comments on the guidelines as part of a public Consultation.

[152] Zerdick, T., in Ehmann/Selmayr, 3rd Edition 2024, Art. 48 para. 1 (for the GDPR).

[153] Art. 32 (3) Regulation (EU) 2023/2854 (EU Data Act).

[154] Art. 32 (5) and Recitals 101 and 102 Regulation (EU) 2023/2854 (EU Data Act).

- publish a general description of the technical, organisational and contractual measures they have taken to prevent access by third-country authorities to non-personal data stored in the EU or to prevent its transfer to third-country authorities.[155]

These provisions – which are often overlooked in the debate on sovereignty requirements[156] – are another piece of the puzzle designed to protect the EU from unauthorised access to personal and non-personal data by third-country authorities. While the provisions of the GDPR already apply, the provisions of the Data Act will be applicable from 11 September 2025. The EU must therefore ensure that any future adoption of sovereignty and other cybersecurity requirements, whether as part of an EUCS or by the EU legislator, does not contradict the aforementioned requirements in the GDPR and Data Act. The above-mentioned sovereignty requirements that have temporarily been provided for in the EUCS go beyond the aforementioned provisions in the Data Act and the GDPR. The Data Act does not regulate in detail which technical, organisational and contractual measures the provider must take, but only mentions general examples such as encryption, audits and checks, while the EUCS sets out more detailed requirements on this. The Data Act also does not stipulate data localisation or the requirement of a headquarters in the EU. When designing the requirements for preventing access, the EU should draw on the experience regarding the effectiveness of the aforementioned provisions in the GDPR and Data Act.

3.5.4 Compatibility with the Regulation on the free movement of non-personal data

Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union (Free Flow of Data Regulation, see cep**PolicyBrief**)[157] prohibits EU Member States from maintaining or imposing new data localisation requirements unless they are justified and proportionate for reasons of public security.[158] Data localisation requirements in this sense are national legal or administrative provisions that require data to be stored or processed in one's own Member State or that hinder the storage or processing of data in another Member State, for example by requiring the use of a local provider or obtaining authorisation.[159]

Data localisation requirements established on the basis of existing Union law remain unaffected by this prohibition. However, the Regulation only aims to improve the free movement of non-personal data within the EU (and not with third countries) by removing "localisation restrictions", eliminating legal uncertainty and thus creating an effectively functioning internal market for cloud services. However, it does not prohibit data localisation in the EU.

3.5.5 Interference with EU fundamental rights?

An obligation for certain essential, important or "critical" EU companies to use only certified cloud services could restrict the entrepreneurial freedom of these companies to freely choose their cloud service provider, as enshrined in Art. 16 of the EU Charter of Fundamental Rights. However, as long as certification remains voluntary, companies are free to use alternative providers that are not certified

[155] Art. 28 (1) Regulation (EU) 2023/2854 (EU Data Act).
[156] Goyet, M., European Commission, Deputy Head of Unit – Cloud and Software, at a Forum Europe event on European Sovereign Cloud Day, available here.
[157] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union; for more details see Hoffmann, A. / Eckhardt, P., Free Flow of Non-Personal Data, see cep**PolicyBrief** 33/2017.
[158] Art. 1 (1) Regulation (EU) 2018/1807.
[159] Cf. Hoffmann, A./ Eckhardt, P., loc. cit. p. 2.

under the EUCS. If certification becomes mandatory in the future – for individual companies or organisations – there would have to be careful examination of the extent to which the obligation to use certified cloud services can be justified. According to the case law of the CJEU, under Art. 52 (1) of the EU Charter of Fundamental Rights, any interference must have a statutory, legally binding basis, i.e. a provision issued by the EU legislator.[160] Although the CJEU has categorised an implementing regulation – as would be the case if the Commission adopted the EUCS – as a "law" within the meaning of Art. 52 (1), CFR,[161] an implementing regulation is not sufficient if the provisions in question permit interference with the fundamental rights of the persons concerned to an extent that requires action by the Union legislator. According to the CJEU, this is the case if the adoption of the provisions requires political decisions that involve the conflicting interests to be weighed up on the basis of an assessment of numerous aspects and therefore fall within the competence of the Union legislator.[162]

Sovereignty requirements involving a high depth of intervention, such as the requirement of strict data localisation in the EU or the exclusive use of providers with headquarters in the EU, would therefore have to be regulated by the EU legislator and not solely by the Commission, unless they are already provided for in the Data Act or the GDPR or covered by the CSA or other EU law. If this is the case or occurs in the future, further examination would be required as to whether the interference – i.e. the obligation to use only certified cloud services – serves legitimate purposes, such as maintaining the functionality of ICT infrastructure operated by important or critical companies and organisations, and could therefore be justified under Art. 52 of the EU CFR. To this end, however, the obligation to use only certified cloud services would have to be suitable and necessary to protect such interests. The sovereignty requirements must firstly therefore be suitable for actually achieving their stated objectives – e.g. protecting sensitive data from unwanted access by third countries or ensuring better enforcement of EU law against cloud service providers. This can be assumed if the sovereignty requirements help to facilitate law enforcement and at least make unjustified access to the data more difficult, even if such access cannot ultimately be completely avoided despite compliance with the sovereignty requirements.

The sovereignty requirements must also be necessary, i.e. no less restrictive measures are available. As part of this proportionality test, the conflicting interests must be weighed up against each other, taking into account all relevant aspects of the individual case. On the one hand, this includes the sensitivity of the data and infrastructure and its need for protection, and on the other, the rationale behind the requirements as well as the disadvantages that EU companies incur from the obligation to use a cloud service certified at a certain assurance level. This will have to be examined for each sovereignty requirement individually and taking them as a whole. For example, an obligation to use providers that store their data exclusively in the EU, have their headquarters there and have no connection to a US company could be disproportionate if only a small amount of sensitive data is processed and the processing of sensitive and non-sensitive data is separated or can be reasonably separated. In this context, it must also be examined how realistic it is to assume that cloud providers operating in the EU will actually be able to evade access by third-country authorities through the requirements intended to ensure their immunity from third-country law, i.e. that they can in practice achieve de facto "immunity" from third-country law. With regard to the USA, this will depend not least on how the US courts

[160] CJEU, Judgement of 4 May 2016, Case C-547/14 – Philipp Morris, ECLI:EU:C:2016:325, para. 149 (“provided for by law”).
[161] CJEU, Judgement of 9 November 2010, Joined Cases C-92/09 and C-93/09 – Schecke, ECLI:EU:C:2010:662, para. 66; see also Jarass, H.,Charta der Grundrechte der EU, 4th Edition 2021, Art. 52 para. 25.
[162] CJEU, Judgement of 5 September 2012, CaseC-355/10 – EP v. Council, C-176/03, ECLI:EU:C:2012:516, para. 77, 76, 84.

assess the attempts of companies to free themselves from US jurisdiction or the US CLOUD Act[163,164], and what consequences the USA will draw from this or what countermeasures it might consider if its laws do not have the desired effect.

3.5.6 Potential conflicts with international trade law

The EU and its individual Member States are members of the World Trade Organisation (WTO); the EU represents the interests of all Member States as agreed in the Common Commercial Policy.[165] In the case of majority decisions, the EU exercises the right to vote for all Member States and thus has 27 votes, and the vote of the EU as an independent WTO member is cancelled. WTO law is principally based on three pillars. The centrepiece of world trade law is the General Agreement on Tariffs and Trade (GATT)[166]; it contains the basic rules for the international trade in goods, the elimination of customs duties and the removal of other non-tariff trade barriers. Its scope of application includes "goods", "merchandise" and "products" and thus all physically tangible items that can be the subject of commercial transactions. This is to be distinguished from trade in services, which falls under the scope of the General Agreement on Trade in Services (GATS)[167] , which forms the second[168] pillar of WTO law.[169] The WHO offers a dispute resolution system for resolving trade disputes. Dispute resolution is initially the responsibility of the Dispute Settlement Body as the arbitrating body; however, the member countries can request the establishment of a Dispute Panel.[170]

Are sovereignty requirements covered by a GATS ban?

GATS covers all services with few exceptions.[171] Cloud computing falls under the category of "computer and related services" and is therefore explicitly covered by GATS.[172] GATS applies to "measures by Members affecting trade in services" (Art. 1 GATS). It is intended to transfer the principles of GATT to the area of services. Not only customs duties and quotas, but also market access restrictions and rules regarding the qualification of service providers are therefore now considered trade restrictions.[173]

---

[163] US Clarifying Lawful Overseas Use of Data Act, H.R. 4943, for text see here. The US CLOUD Act also obliges, under certain conditions, cloud service providers with connections to the USA to disclose communication data that is stored outside the United States but is under their "control". For more details, see Hoffmann, A. (2021), Inadmissibility of data transfer to the USA, see cep**Study**.

[164] See also Propp, K. (2022), European Cybersecurity Regulation Takes a Sovereign Turn, available here.

[165] Miederer, K., Der Beitritt zur Welthandelsorganisation und zur Europäischen Union, Ein Vergleich der angewandten Verfahren und Kriterien, Universität Bremen 2002.

[166] WTO, General Agreement on Tariffs and Trade, signed on 30 October 1947, entered into force on 1 January 1948, as amended in 1994, available here.

[167] WTO, General Agreement on Trade in Services (GATS), available here.

[168] The third pillar is the TRIPS Agreement – not relevant here – Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), available here.

[169] Deutscher Bundestag (2019), Gutachten des Wissenschaftlichen Dienstes, Sachstand, Zur Geltendmachung nationaler Sicherheitsinteressen beim Aufbau des 5G-Netzes, available here.

[170] For more details, see WTO, Dispute Settlement System Training Module, paras. 3.1 and 3.3. See also Wikipedia, Dispute Settlement Body.

[171] World Trade Organisation, Services: Services Sectors, see here.

[172] World Trade Organisation, Services: Sector by Sector, Computer and related services, see here; differentiating by functionalities of the cloud service Willemyns, I. (2008), GATS Classification of Digital Services – Does 'The Cloud' Have a Silver Lining?, see here. Because cloud services utilise telecommunications networks, the obligations and market openings of the EU in this area may also be relevant.

[173] Hofmann, R., Skript Internationales Wirtschaftsrecht WS 2013/14, Teil 3, Das WTO/GATT-System, § 8 Grundprinzipien des GATS, p. 2, available here.

One of the key principles of GATT is that of national treatment.[174] It obliges the member countries to treat foreign goods in the same way as domestic goods once they have been imported.[175] As part of GATT's general prohibition of discrimination, it serves to create a level playing field and at the same time prevent protectionism.[176] Accordingly, the principle of national treatment in GATS prohibits discrimination against a foreign service in favour of a similar domestic service.[177] Discrimination exists if the measures in question change the competitive conditions in favour of domestic service providers. This covers not only legal but also de facto discrimination against foreign providers.[178] There is a separate agreement for public procurement within the framework of the WTO because public procurement is explicitly excluded from the main areas of deregulation under GATT and GATS. The Government Procurement Agreement (GPA)[179] also stipulates national treatment and non-discrimination for public contracts. However, as a "plurilateral" agreement, it does not apply to all WTO members, but only to the GPA signatories, including the EU, USA and Japan.[180] The EU has established exemptions in the telecommunications sector, among others.[181] Citing national treatment, the former US ambassador to the WTO Pagán expressed concerns and called on the EU to review the EUCS. She criticised that the EU had assumed obligations for cloud services under the GPA and was therefore obliged to ensure non-discriminatory access to the relevant services.[182] As the GPA also regulates similar principles and exceptions[183] as GATT and GATS, this cep**Input** will not deal with them separately.

In contrast to GATT, the principle of national treatment under GATS does not generally apply to all WTO member countries. In this respect, GATS distinguishes between general obligations that apply to all WTO members in Part II[184] and "specific" obligations in Part III, which only apply to those member countries that have explicitly undertaken to fulfil them. This includes the elimination of market access restrictions (Art. XVI)[185] and the principle of national treatment (Art. XVII).[186] Market access and national treatment therefore only apply within the framework of the specific obligations that the countries have entered into in their schedules. A right to market access, i.e. to access the market of the other member country (in this case the EU), therefore only exists insofar as this is regulated in the aforementioned schedules of specific commitments of that country.[187]

The extent to which the EU and the EU Member States have assumed general and sector-specific obligations under GATS that also apply to cloud services as a "newer" type of service requires a complex examination[188], which will not be undertaken here. The same applies to the question of which

[174] Art. III GATT 1994.
[175] JuraForum, GATT: Definition & meaning in international trade and commercial law, see here.
[176] Hofmann, R., Part 3 § 7, loc. cit. p. 3.
[177] Fischer, K. (2022), Die WTO und der Dienstleistungshandel, see here.
[178] Fischer, K. (2022), loc. cit., cf. also Hofmann, R., Part 3 § 8, loc. cit., p. 6.
[179] The latest revised version of the agreement from 2012 is available here.
[180] Bauer, N. (2022), WTO und öffentliche Beschaffung, available here.
[181] See Final Report of the Select Committee "Globalisierung der Weltwirtschaft – Herausforderungen und Antworten", BT-Drucks. 14/9200 of 12 June 2002, para. 3.3.3.1.7, available here.
[182] Pagán, M. (2023), U.S. Opening Remarks at the Trade Policy Review of the European Union, available here; see also Propp (2023), Oceans apart: The EU and US Cybersecurity Certification Standards for Cloud Services, available here.
[183] Art. III of the Agreement on Government Procurement provides for similar exceptions to protect public order, human life and health and essential security interests. These exceptions are discussed in more detail below in the context of GATS
[184] These include, for example, the principle of most-favoured-nation treatment (Art. II GATS) and transparency obligations (Art. III GATS).
[185] Text available here.
[186] Text available here. See on this Hofmann, R., Part 3 § 8, loc. cit., p. 2.
[187] The schedules are therefore of crucial importance for the question of market access, see Fischer, K. (2022), Die WTO und der Dienstleistungshandel, cf. here.
[188] Well illustrated in Ungphakorn, P. (2021), Technical note: what are schedules of commitments in services?, Trade β Blog, see here.

potentially relevant exceptions to the obligations have been explicitly included in the schedules. For the purposes of this cep**Input**, it should therefore be assumed, subject to closer examination, that the EU or its Member States have assumed obligations under GATS which in principle oblige them to open up their market and provide national treatment for cloud service providers.

It could be argued that sovereignty requirements that oblige cloud service providers to localise data in the EU or to have its registered headquarters and global head office in the EU are in conflict with the desired liberalisation of trade in services because they may unjustifiably restrict the access of third-country providers to the EU cloud market or place them at a disadvantage compared to European providers. This view is shared by 26 industry groups, who declared in a joint letter[189] to the EU Member States in June 2024 that the strict sovereignty requirements temporarily provided for in the EUCS discriminate against major US cloud service providers such as Amazon, Alphabet (Google) and Microsoft.[190] Back in May 2024, the American Chamber of Commerce to the EU and twelve other industry associations had already pointed out in a joint statement that the requirements for company ownership, data localisation and immunity from non-EU law would prevent the vast majority of non-European cloud service providers from offering their services to customers in the EU who want to use cloud services certified at the highest level of assurance.[191] Other voices have also pointed out that mandatory data localisation measures hinder the flow of data and therefore represent barriers to trade, arguing that they increase compliance costs for foreign service providers and limit their market access opportunities. According to them, end consumers and companies in the EU that (want to) use cloud services would at the same time have limited access to competitive foreign services and would lose significant business opportunities as a result.[192]

On the other hand, governments are increasingly using strong political arguments to justify data localisation. They either generally propagate the need for strong sovereign control, like China and Russia, or argue more specifically that their measures are necessary to ensure data protection and network security, to prevent cybercrime, to support domestic law enforcement and to protect intellectual property. Few countries admit that there are often protectionist reasons behind these measures.[193]

Justification by GATS exceptions?

GATS provides for various **exceptions** that, under certain circumstances, allow member countries to deviate from its principles, such as the requirement of market access and non-discrimination. They are intended to enable member countries to ensure the protection of important goods despite the fundamental restriction of their room for manoeuvre by their obligations under trade law.[194] However, GATS predates the Internet and there is therefore legal uncertainty as to the extent to which its provisions can be used to solve the challenges of the digital age.[195]

---

[189] The signatories to the letter included the American Chamber of Commerce in the Czech Republic, Estonia, Finland, Italy, Norway, Romania and Spain, the European Payment Institutions Federation (EPIF) and the Association of German Banks, see Chee, F. (2024), EU cybersecurity label should not discriminate against Big Tech, European groups say, see here.

[190] Chee, F., (2024), loc. cit.

[191] Joint industry statement on the need for a swift adoption of the EU Cybersecurity Certification Scheme for Cloud Services without sovereignty requirements, see here.

[192] Thus – generally for digital services – Mishra, N. (2019), Privacy, Cybersecurity and GATS Article XIV: A New Frontier for Trade and Internet Regulation?, p. 3 and 6f., cf. here.

[193] Mishra, N. (loc. cit.), p. 8.

[194] Deutscher Bundestag (2019), Gutachten des Wissenschaftlichen Dienstes, p. 6, see here on GATT; this also applies to GATS.

[195] More on this issue Mishra, N. (2019), loc. cit., p. 13. So far, there is no interpretative guidance for digital trade commitments as there have been no related disputes under recent preferential trade agreements, see Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, p. 397 (410), see here.

Sovereignty requirements designed to protect data, privacy and cybersecurity could initially fall under the **general exceptions to GATS**.[196] According to this provision, member countries may, under certain conditions, take measures that are necessary to maintain public order (Art. XIV (a) GATS). They may also take necessary measures to ensure compliance with laws relating to safety or to the protection of privacy in relation to the processing and dissemination of personal data and to the protection of confidentiality of personal records and accounts (Article XIV(c) GATS). Data protection is therefore explicitly recognised as a legitimate objective. This suggests that a restriction to locations in countries with adequate data protection, for example, may be a WTO-compatible measure. However, the public order exception can only be invoked if there is a genuine and sufficiently serious threat to one of the fundamental interests of society. To the extent that the EU can argue that the sovereignty requirements affect fundamental interests of EU citizens, Article XIV(a) GATS could also be used to justify cybersecurity measures.[197] For example, it could cover measures to combat security threats on the Internet of Things ("IoT"), which pose a "serious threat" to the security of all homes connected via smart gadgets.[198]

The general exceptions to GATS are intended to strike a balance between the obligations to liberalise international trade and a member's national understanding of privacy and cybersecurity as objectives of data localisation measures.[199] However, specifically which measures are "necessary" can only be determined by a tricky weighing up of these conflicting objectives and an assessment of complex technical issues.[200] "Necessary" means that no less trade-restrictive alternative that fulfils the same purpose is "reasonably available". The trade-off is complicated by the fact that localisation measures often pursue several objectives and/or can both protect privacy and benefit the domestic digital economy at the same time. Legitimate reasons may also conceal protectionist intentions.[201] However, the exception must not be invoked for the purpose of misuse, i.e. the measures must be implemented and enforced in "good faith"[202] in a coherent manner and must not constitute arbitrary or unjustifiable discrimination or a disguised restriction on trade.[203] They must not therefore primarily serve protectionist purposes.

Ensuring the free flow of data is important for the use of the internet as a platform for the exchange of digital services. On the other hand, data protection and cybersecurity are also fundamental prerequisites for maintaining the stability of the internet and enabling a trustworthy environment for cross-border data traffic and are therefore increasingly recognised as a prerequisite for facilitating digital trade.[204] Some experts therefore believe that a WTO panel is likely to give high priority to these objectives due to their strategic importance and the risks in the event of their absence in a trade dispute over data localisation.[205] In their view, a data localisation measure could be justified, for example, if a country prevents the transfer of data to countries with a very poor track record in the area of

[196] Mishra, N. (2019), loc. cit., p. 12f.
[197] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, p. 397*(413)*, cf. here.
[198] Mishra, N. (2019), loc. cit., p. 17.
[199] Mishra, N. (2019), Privacy, Cybersecurity and GATS Article XIV: A New Frontier for Trade and Internet Regulation?, p. 5, cf. here.
[200] Cf. Mishra, N. (2019), loc. cit., p. 12 and 30.
[201] Mishra, N. (2019), loc. cit., p. 3.
[202] Mishra, N. (2019), loc. cit., p. 25.
[203] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, p. 397 *(414)*, cf. here.
[204] Cf. Mishra, N. (2019), loc. cit., p. 18 and 26.
[205] Cf. Mishra, N. (2019), loc. cit., p. 18.

cybersecurity or data protection, e.g. if governments are known to force companies to hand over data coercively.[206] Conversely, certain forms of localisation may be unnecessary if less sensitive, non-personal or anonymised data sets are involved or if the technology underlying a digital service is highly secure and robust.[207] Other authors point out that the fulfilment of the requirements of the – narrowly interpreted – GATS exceptions represents a relatively high hurdle for WTO members and that the "success rate" for invoking the exceptions has been rather low.[208] However, complaints are generally only lodged if the chances of success are high. Whether EU sovereignty requirements are actually at risk of being challenged before a panel is, however, an open question and is considered rather unlikely by some.[209] However, the EU cannot rely on this.

In any case, the panels have a margin of discretion when assessing the legality of data localisation measures.[210] To date, there is also no WTO panel case law on the privacy/data protection exception under Article XIV(c) GATS[211] that could limit this discretion. There is still no consensus among WTO members on the role of cybersecurity and data protection in international trade law. There is also a lack of specific international laws, norms or standards on cybersecurity and the protection of privacy. Experts are divided on the most effective standards for data protection and cybersecurity. Therefore, the ability of WTO tribunals to find a balance between trade liberalisation and legitimate national interests is limited, according to experts, and the panels will be tested to their limits when it comes to deciding on the legitimacy of such measures.[212]

In addition to the general exceptions, GATS also provides **for exceptions to protect national security interests** (Art. XIV bis GATS).[213] Accordingly, the GATS obligations do not prevent Member States from refusing to provide information which they "consider" to be contrary to their "essential security interests" and from taking measures which they "consider" to be necessary to protect their "essential security interests". Consequently, GATS leaves it up to the respective WTO member country to assess whether essential (national) security interests are threatened .[214] The concept of "essential security interests" is narrower than that of "security interests" and refers to the essential functions of the state in relation to the protection of its territory and population from external threats and the maintenance of law and public order. Each member country determines what its essential security interests are and what measures are necessary, at least as far as possible.[215] Nevertheless, the utilisation of the security exception is not completely self-determined.[216] In 2019, a WTO panel issued a landmark ruling in a dispute between Russia and Ukraine[217] after Russia invoked the security exception[218] and took trade-

[206] Mishra, N. (2019), loc. cit., p. 19.
[207] Mishra, N., p. 27.
[208] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, p. 397 (415), cf. here.
[209] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, p. 397 (415, 419), cf. here.
[210] Mishra, N. (2019), loc. cit., p. 28.
[211] Burri, M. / Kugler, K., Regulatory autonomy in digital trade agreements, Zeitschrift für Internationales Wirtschaftsrecht, 2024, p. 397 (412), cf. here.
[212] Mishra, N. (2019), loc. cit., p. 12f. and 29.
[213] Art. XXIII of the Agreement on Government Procurement also provides for a "security exception".
[214] Deutscher Bundestag (2019), Gutachten des Wissenschaftlichen Dienstes, loc. cit., p. 6, on the substantively identical Art. XIV bis GATT.
[215] Burri, M. / Kugler, K., loc. cit., p. 422; in this respect also Peng, S., Cybersecurity Threats and the WTO National Security Exceptions, Journal of International Economic Law, 2015, A. 449ff., which derives this from the interpretation of the text (p. 434) and context (p. 464) of Art. XIV GATS, cf. here.
[216] See already Peng, S., loc. cit., pp. 464 and 466f.
[217] WTO Dispute Settlement (DS)512: Russia – Measures Concerning Traffic in Transit, see here.
[218] In this case Art. XXI GATT, which, however, is largely comparable to Art. XIV GATS.

restrictive measures to protect its national security.[219] The panel ruled that measures taken by WTO members on the grounds of national security are at least objectively verifiable through WTO dispute settlement procedures. In doing so, it explicitly rejected Russia's argument – which was also put forward by the USA in several cases – that measures to protect essential security interests were at the sole discretion of the member countries and that a decision by a WTO panel on this would violate their national sovereignty.[220]

The EU's sovereignty requirements must therefore serve to protect its "essential security interests", at least from the perspective of the EU or its Member States. Some experts point out that the importance of cybersecurity has changed in recent years. While cybersecurity primarily serves to maintain the functionality of network and information systems[221], the concept of information security is in their view intended to protect the confidentiality of (personal) data and prevent its disclosure. They argue that while information security does not necessarily fall within the scope of national security[222], the pursuit of cybersecurity has recently become more and more of a national security issue. In any case, it remains unclear at what point the risk becomes a danger to which "essential interests". In addition, the EU or its Member States would have to be able to invoke an emergency situation in order to apply the security exception and be authorised to take measures[223], namely either that it is "in time of war" or that there is another "emergency in international relations". In the Russia-Ukraine case, the panel defined such an "emergency in international relations" as "a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state".[224] It claimed that whether such a situation existed can be objectively reviewed by a panel, as can be the question of whether the challenged measure was taken "at the time of" such an emergency and whether there was a plausible relationship between the conflict and the trade-restrictive measure taken.[225] If the EU wants to invoke this exception, it will therefore have to argue that it is currently already in such a crisis. In doing so, it must bear in mind that the panel did not consider mere political or economic differences between the members to be sufficient, of themselves, to constitute an emergency in international relations.[226] At the end of 2022, in the legal dispute over US tariffs on steel and aluminium, a WTO panel again had to decide on the conditions of the security exception. US President Trump invoked this exception in 2018 to justify the additional US tariffs he introduced on steel and aluminium.[227] However, the panel did not consider a state of emergency to exist, as there was no impact on international relations comparable to a war.[228] The USA did not recognise the panel's decision

[219] The background to the proceedings was the blockade of trade, transiting through Russia, between Ukraine, Kazakhstan and the Kyrgyz Republic, in response to the escalation of events in Ukraine following the political unrest in 2014. As a result, however, the panel considered the Russian measures to be covered by the security exception, see Reinsch, W./ Caporal, J. (2019), Die erste Entscheidung der WTO zur nationalen Sicherheit: What does it mean for the United States? See here.

[220] Reinsch, W./ Caporal, J. (2019), loc. cit.

[221] Art. 2 No. 1 , Regulation (EU) 2019/881.

[222] Peng, S. (2015), Cybersecurity Threats and the WTO National Security Exceptions, Journal of International Economic Law, 2015, A. 449 ff., loc. cit., p. 449 (469), cf. here.

[223] Art. XIV bis lit. b ii) GATS.

[224] Reinsch, W./ Caporal, J. (2019), The WTO's First Ruling on National Security: What Does It Mean for the United States?, see here.

[225] Reinsch, W./ Caporal, J. (2019), loc. cit.

[226] Reinsch, W./ Caporal, J. (2019), loc. cit.

[227] Reinsch, W./ Caporal, J. (2019), loc. cit.

[228] See paragraph 7.139 -7.149 of the Panel Report on WTO Dispute Settlement (DS) 544 of 9 December 2019, see here.

and lodged an appeal against it at the end of January 2023.[229] In view of the USA's current efforts to block[230] WTO dispute settlement, a decision by an appellate body is unlikely in the foreseeable future.

Whether the EU's sovereignty requirements can be justified by invoking one of the security exceptions is an open question. It is becoming apparent that national security could increasingly become a pretext for protective measures in international trade.[231] However, trade interests must not be "relabelled" as essential security interests.[232] The security exemptions only apply to a limited number of scenarios, most of which, according to experts, are not applicable to current cybersecurity measures. There is also uncertainty as to which measures the exemptions cover in order to counter imminent cyber and other threats.[233] Questions relating to the burden of proof also remain unanswered. The outcome of a possible dispute resolution procedure would therefore be uncertain.[234]

Political considerations

Irrespective of the legal outcome of such a consideration, it is also unclear whether a complaint would actually be lodged with the WTO or whether a WTO panel would have to make a decision in which the panel would have to weigh up the national security interests of the EU or its Member States against the desired trade liberalisation. Historically, the national security exception has been applied rather cautiously.[235] The WTO has refused to strike a balance between the interests of international trade and national security and sidestepped the questions put to it regarding justification under the security exception. To date, there is only limited relevant WTO case law on measures taken to strengthen national security. In addition, the case law is not clear because the ambiguity of the exceptions for national security opens up a lot of room for legal interpretation. For precisely this reason, not only was the ambiguity intentional in terms of negotiation history, but it can also be surmised that in the past WTO members have obviously tried to avoid a WTO ruling on security exemptions. They tended to be reluctant to bring issues to the WTO which they considered to be important national security issues. This is because it can make sense to leave the interpretation of the security exemptions vague if the members are not sure which side they will be on in a dispute.[236] Invoking the WTO exceptions in trade disputes related to cybersecurity may also lead to undesirable outcomes as the panels would have to deal with highly sensitive issues.[237] The panel rulings in the Russia-Ukraine conflict and in the trade dispute over US tariffs on steel and aluminium could provide an indication of how future WTO panels might deal with other disputes in which one party invokes the security exception.[238] However, if the circumstances differ, other panels may also view the issue of national security differently.[239] Overall, the WTO is probably still at the beginning of its deliberations on the issue of national security.[240] In all of this, there is also always the risk that decisions in which the panels go too far in restricting the member countries'

[229] See here.
[230] Hoffmann, M. (2024), Blockade der WTO-Streitschlichtung: Wie geht es weiter? See https://www.gtai.de/de/trade/wto/zoll/blockade-der-wto-streitschlichtung-wie-geht-es-weiter--244124; Kessler, D. (2021), Der Konflikt um die WTO-Streitschlichtung, Wissenschaftlicher Dienst des Deutschen Bundestags, see here.
[231] As already surmised by Peng, S. (2015), loc. cit., p. 449 (450).
[232] Reinsch, W./ Caporal, J. (2019), loc. cit.
[233] Burri, M. / Kugler, K., loc. cit., p. 422.
[234] Likewise Propp, K. (2022), European Cybersecurity Regulation Takes a Sovereign Turn, cf. here.
[235] Peng, S., Cybersecurity Threats and the WTO National Security Exceptions, Journal of International Economic Law, 2015, A. 449 (459), cf. here.
[236] Peng, S., Cybersecurity Threats and the WTO National Security Exceptions, loc. cit.
[237] Burri, M. / Kugler, K., loc. cit., p. 422.
[238] Reinsch, W./ Caporal, J. (2019), loc. cit.
[239] Reinsch, W./ Caporal, J. (2019), loc. cit.
[240] Reinsch, W./ Caporal, J. (2019), loc. cit.

ability to utilise the security exception will be seen by the latter as an unacceptable violation of national sovereignty and lead to members withdrawing from the WTO.

The example of the USA also shows that countries can be on both sides of trade disputes relating to cybersecurity: on the one hand, the US Chamber of Commerce is resisting possible EU sovereignty requirements in the context of cybersecurity certification with the argument that these could put US-based hyperscalers at a disadvantage on the European market.[241] On the other hand, the United States wants to protect itself and its citizens by banning or imposing trade sanctions on the use of Chinese technology in telecommunications.[242] Conversely, following the Snowden revelations, China banned its regulatory authorities from installing Microsoft's Windows 8 operating system on new computers due to cybersecurity concerns.[243] The arguments often seem to be similar: in addition to alleged discrimination, it is argued that the measure in question could or will seriously affect competition in the sector concerned. If the restrictions are perceived as protectionism, there is also a risk that the affected states will retaliate with their own security measures against technologies or services from the other state.[244] The EU must not ignore this risk. Nevertheless, it is evident that the problem – wanting to make use of exemptions from WTO obligations for one's own protection, but not allowing other states to do the same, or provoking sanctions from other states with one's own measures – ultimately affects several, if not all, states.

Looking at the situation regarding cloud services, it becomes clear that other countries also have their own programmes in place to protect sensitive data stored in the cloud. With its Federal Risk and Authorisation Management Program (FedRAMP)[245], for example, the USA has introduced a government-wide programme that offers a standardised approach to security assessment, authorisation and control for cloud products and services that may be used by public authorities. At the highest level of "High Baseline", this programme also requires localisation of data and services, limited to US territory or geographic locations under US jurisdiction, to protect the most sensitive US government data in cloud computing environments.[246] Critics of the EUCS, on the other hand, argue that its blanket data localisation and immunity requirements are not comparable to the more nuanced, risk-based and non-discriminatory system of FedRAMP, which limits data localisation requirements to certain systems in the high-risk category and allows non-US-based providers even at the high criticality level.[247] However, according to a law being proposed by the US Department of Defence, the US is apparently also considering changing the conditions to the effect that cloud services with FedRAMP High must physically store all government data in the United States or its peripheral areas or on government property.[248] Regardless of the differences between the various national programmes, the example shows that ensuring the (cyber)security of cloud services and sensitive data is not just a European need, but a widespread international one.

---

[241] Peng, S., loc. cit., p. 449 (455f.).
[242] See for example Daum, T. (2024), Missing Link: Huawei-Sanktionen – Der Schuss geht nach hinten los, see here.
[243] Peng, S., loc. cit., p. 449 (450).
[244] For example, the argument of critics of a US law that restricted the public procurement of Chinese IT by selected US federal agencies, cf. Peng, S., loc. cit., p. 455f.
[245] https://www.fedramp.gov/.
[246] United States Government (2020), An Update to FedRAMP's High Baseline SA-9(5) Control, see here.
[247] Propp, K. (2023).
[248] Schneider, G./ McGiff, T. (2024), Proposed FAR Rule on Data Localization Would Undermine U.S. Cybersecurity, Competitiveness, see here.

3.6 Interim conclusion

3.6.1 (Political) economic perspective

The EU's increased efforts to establish and promote EU markets for cloud services that are both cybersecure and ensure digital sovereignty are understandable and comprehensible from a geopolitical and security policy perspective. Not least the further increase in uncertainty in the geopolitical situation following Donald Trump's election victory makes it clear that additional efforts are needed here. However, whether the establishment of a European cybersecurity certification scheme for cloud services (EUCS) with specific "sovereignty requirements" is a sensible, suitable and effective step from a (political) economic perspective is and remains controversial. Ultimately, the success of any EUCS depends on whether it is considered credible and, although designed as a voluntary scheme, is actually applied in practice. At present, supporters and opponents of sovereignty requirements are seemingly irreconcilable, both in the case of political decision-makers and in the case of the economic players concerned. This makes it at least doubtful that an EUCS with sovereignty requirements will meet with broad acceptance in practice. Before such an EUCS is adopted, it is therefore important to dispel or at least mitigate these doubts. Otherwise, the EUCS certification scheme will not gain widespread acceptance in competition with alternative instruments, such as private seals of approval, labels or industry standards that promise to inform (potential) cloud users about the cybersecurity properties of cloud services. It could be argued that the voluntary nature of the scheme means that all market players concerned are free to choose and, even if sovereignty requirements are included in the scheme, they are free to use cloud services that do not fulfil these requirements. However, the more inclined the EU or the Member States are (in future) to oblige certain players – such as operators of critical infrastructures or public administrations – to use cloud services certified exclusively in accordance with an EUCS which contains strict sovereignty requirements, the more important it will be for political decision-makers to dispel any doubts about the rationale and advisability of sovereignty requirements. If the aforementioned doubts persist, these stakeholders will either be forced to use cloud services that do not or only partially meet their (cybersecurity) expectations, or they may refrain from using cloud services at all. If, in the future, an EUCS with sovereignty requirements is adopted that does not meet with broad acceptance, it should not be made mandatory to use only EUCS-certified services, even for individual players. Users should also be allowed to use competing instruments as an alternative.

3.6.2 Legal perspective

Regulating sovereignty requirements of the type described above in an EUCS is tricky from a legal perspective because it would not simply be an apolitical clarification of the provisions of the EU Cybersecurity Act (CSA). The EU should in fact be aiming to regulate strict sovereignty requirements, that go beyond the existing provisions in the Data Act, the GDPR and other EU legislation, through the EU legislator (i.e. by way of a Regulation or a Directive) and not within the framework of an EUCS at the level of an implementing regulation. It should create a legal basis for controversial sovereignty requirements such as the residency requirement, data localisation and corporate control, or requirements intended to ensure the immunity of cloud providers from third-country law. Such requirements can have far-reaching effects on the cloud market in the EU and international trade, which is why their establishment is an essential fundamental decision which, from a legal perspective, is reserved for the EU legislator. With the help of an EU legislative act, such requirements could be democratically legitimised and encroachments on fundamental rights associated with the sovereignty requirements could be justified if they are proportionate.

The EU may be able to base the (re)regulation of cybersecurity and sovereignty requirements on the competence to harmonise the internal market under Art. 114 TFEU. Depending on the scope and design of such regulation, however, the EU might principally have to use the legislative competence for the harmonisation of the trade in services under Art. 53 (1) in conjunction with Art. 62 TFEU, which is specific to the fundamental freedoms, in order to coordinate the different Member States' sovereignty requirements for cloud services by means of an EU Directive. Since, by taking legislative action, the EU will be interfering with the competence of Member States to regulate their cybersecurity and other security interests in a self-determined manner, and this can lead to a reduction in the level of protection in the Member States, it must respect the principles of subsidiarity and proportionality when regulating the requirements. A high level of cybersecurity across the EU is generally best achieved at EU level. However, in order to protect important national interests such as public security, national defence and public order, Member States should be allowed to regulate or maintain stricter national requirements and certification schemes. This applies even more to requirements designed to ensure the protection of the national security of the Member States. In the area of national security – which is to be understood narrowly and concerns the security of a state in the narrower sense –, the sole regulatory competence remains with the Member States, which is why the EU must exclude this area from its legislation.

In order to avoid contradictions and legal uncertainty, the EU must also ensure that sovereignty and other cybersecurity requirements which it regulates are harmonised and aligned with the provisions in the Data Act, the GDPR and other legal acts such as the NIS II Directive and the AI Act.[249]

The EU should design any sovereignty requirements in such a way that they cannot be successfully challenged before a WTO panel, or it should at least minimise this risk as far as possible. In doing so, the EU should ensure that the criteria are designed in such a way that they cannot be misunderstood as an overtly or covertly protectionist trading arrangement.

As other countries are also increasingly claiming exemptions from international free trade on the grounds of national security and sovereignty and there is a lack of clarity as to how existing international trade law should be applied to digital services such as cloud services, the EU and its Member States, together with their trading partners, must make a strong commitment to agreeing updated international rules for modernised, digital global trade law. In doing so, they should try to establish customised exceptions for data and cybersecurity and "national sovereignty" at international level on the basis of reciprocity and equality, or find some other consensus. In this context, it should also be clarified whether exceptions to free trade should be implemented in future not only to protect personal data, but also to protect cybersecurity and trade secrets and sensitive know-how. In bilateral terms, the Trade and Technology Council should also (continue to) be used as a forum for discussion on mutual approaches to the provision of cloud services in the private sector and to the public sector.[250] In the increasingly complex field of tension between international free trade and state security interests[251], it is essential to find a consensus-based balance in order to master the challenges of the data-driven economy.

[249] Opinion of the Netherlands on the non-paper by DE, ES, FR and IT on the EUCS requirements for immunity from non-EU laws (2021), cf. here.
[250] Propp, K. (2022), European Cybersecurity Regulation Takes a Sovereign Turn, 12 September 2022, available here.
[251] Peng, S. (2015), loc. cit., p. 449 (450).

3.6.3 What follows from this analysis?

The foregoing analysis indicates: The controversy regarding the rationale and advisability of sovereignty requirements (within an EUCS) and the risk of a lack of acceptance of an EUCS containing such requirements, as well as possible legal pitfalls affecting the solution now being considered to regulate sovereignty requirements within the framework of an EUCS and to make this mandatory for certain actors in the future, suggest that a new attempt is needed to find ways out of the deadlocked debate. The following section will outline some possible ways out of the difficulties.

4 Ways out of the certification dilemma

Even after years of discussion, the EU Commission, the EU legislator, ENISA and other bodies and stakeholders involved in the development of an EUCS have not been able to agree on a final version of an EUCS – with or without sovereignty requirements – and a compromise that satisfies all sides does not appear to be in sight at present. It is therefore time to think about alternative approaches. The following section will set out possible ways out of this impasse and provide a step-by-step analysis. This will include the ideas presented by Mario Draghi in his report on strengthening competitiveness[252] and by the Commission in its "Mission Letter" to Henna Virkkunen[253], the new Vice President for "Technological Sovereignty, Security and Democracy".[254]

4.1 Adoption of the EUCS without sovereignty requirements

The EU Commission should now swiftly adopt the EUCS, regardless of the ongoing discussions on sovereignty requirements. A further delay would be counterproductive. Even if the EUCS is not a "panacea" and fails to fully address all the reasons for market failure in the markets for (cyber-secure) cloud services (see section 2.3), it can still revitalise the market for cyber-secure cloud services by reducing information asymmetries and strengthening the confidence of potential users in the services. This alone would go some way towards strengthening the cybersecurity of cloud solutions. It would also create legal and planning certainty for the players concerned and establish a standardised solution for the internal market. Sovereignty requirements for cloud services should be avoided due to legal concerns (see section 3.5 and cep**PolicyBrief**), but also due to the current political disagreement and the risk of a lack of acceptance of an EUCS involving such requirements. Instead, such requirements should be decided at political level – i.e. by the European Parliament and the Council – and not as part of the definition of technical specifications in the context of an implementing act.

4.2 Revision of the EU Cybersecurity Act (CSA)

The EU Cybersecurity Act (CSA, see cep**PolicyBrief**) came into force in spring 2019, establishing a framework for certifying the cybersecurity of ICT products, services and processes at EU level.

---

[252] EU Commission (2024a).

[253] EU Commission (2024b), Mission Letter from Ursula von der Leyen, President of the European Commission to Henna Virkunnen, Executive Vice-President-designate for Tech Sovereignty, Security and Democracy, 17 September 2024.

[254] In her answers to specific questions from MEPs ahead of her hearing in the European Parliament on 12 November 2024, Henna Virkunnen commented on the future of an EUCS as follows "*I welcome the voluntary EU Cybersecurity Certification Scheme for Cloud Services (EUCS), as it will increase transparency on the security level of cloud services. Once in place, it will address the current fragmentation in certification and lower the financial barriers for providers to offer secure cloud solutions across the EU. At the same time, besides technical requirements, I am conscious of security challenges posed in the current geopolitical context. These challenges would have my attention when working on the different cloud initiatives under my tenure.*" [European Parliament (2024), Questionnaire to the Commissioner-designate, Henna Virkunnen, Executive Vice-President for Tech Sovereignty, Security and Democracy].

However, this cybersecurity certification framework has not proven to be sufficiently efficient in practice and there have been repeated delays in the adoption of EU certification schemes. The CSA stipulates that the Commission had to carry out an assessment of the "impact, effectiveness and efficiency" of the cybersecurity certification rules by the end of June 2024.[255] It must submit the conclusions of this evaluation to the European Parliament and the Council, among others.[256] Even though the Commission has not yet published its conclusions, it already began evaluating the legislative act in February 2024 as part of a consultation process.[257] Furthermore, Henna Virkkunen, the new EU Vice-President for "Technological Sovereignty, Security and Democracy", was tasked in her "Mission Letter" with improving the process of adopting European cybersecurity certification schemes in the legislative period that has now begun in order to strengthen cybersecurity[258]:

"You will contribute to strengthening cybersecurity to protect our industries, citizens and public administrations against internal and external threats, ***notably by improving the adoption process of European cybersecurity certification schemes****."*[259]

In its work programme for the year 2025, the Commission announced to present a “digital package” for Q4 2025. While the package will tackle multiple issues, like the consistency of the digital acquis of the EU, it most likely will also deal with a revision of the CSA including its cybersecurity certification framework.[260] Moreover, in its new European Internal Security Strategy named “Protect EU”[261], the Commission declared that it will “propose to improve the European Cybersecurity Certification Framework (ECCF) to ensure that future certification schemes can be adopted in a timely manner and respond to policy needs”. Also, the Commission wants to “look more broadly at the security and resilience of ICT supply chains and infrastructure” as well as to “take action [potentially apart from the CSA revision] to encourage critical entities to choose cloud and telecom services which offer an appropriate level of cybersecurity, taking into account not only technical risks but also strategic risks and dependencies”.[262]

Furthermore, on 11 April 2025, the Commission issued a consultation on a future revision of the CSA, declaring in an accompanying “call for evidence” that, with regard to the certification framework “there is room for improvement regarding the adoption process, its agility and effectiveness, the clarity and allocation of roles and responsibilities of various actors throughout this process and the maintenance phase of certification schemes” and “more clarity is needed as regards the risks covered by the ECCF, as well as further consideration of how to address the challenge of non-technical risk factors”. In particular, the Commission considers – as most viable policy options - to propose “targeted changes to clarify the [certification] framework and to formalise procedures regarding the maintenance phase

[255] Art. 67 (1) – (3) Regulation (EU) 2019/881.
[256] Art. 67 (4) Regulation (EU) 2019/881.
[257] EU Commission (2024c), Consultation, Evaluation of the Cybersecurity Act, 13 February – 5 March 2024, see here.
[258] EU Commission (2024b).
[259] On 6 December 2024, the Council called for further improvements and measures with regard to the development of EU cybersecurity certification schemes. In conclusions on ENISA, it "stresses" that Member States and industry are "concerned" about the lengthy processes involved in developing certification schemes. It "urges" the Commission to find leaner, more transparent and faster approaches to developing such schemes. This will be taken into account in the planned revision of the CSA. The Council also "recalls" that ENISA and the Commission should consult all relevant stakeholders "in a timely manner" [Council (2024), Conclusions on ENISA, Transport, Telecommunications and Energy Council, Telecommunications, 6 December 2024, available here].
[260] EU Commission (2025a), COM(2025) 45, Commission work programme 2025, Moving forward together: A Bolder, Simpler, Faster Union, Annex 1, 11 February 2025.
[261] EU Commission (2025b), COM(2025) 148, Communication on ProtectEU: a European Internal Security Strategy, 1 April 2025, p. 13, see here.
[262] EU Commission (2025b), loc. cit., p. 13.

of certification schemes", and/or to "repeal the CSA and proposing a comprehensive regulatory intervention". Such intervention would strive for enhanced "efficiency of the ECCF, extending its scope and addressing ICT supply chains security challenges, including non-technical risk factors".[263]

In any case, the envisaged revision of the CSA will be a good opportunity to revise the requirements for cybersecurity certification. The following adjustments and considerations would be particularly useful in this revision:

- Clear focus on strengthening cybersecurity: Strengthening cybersecurity should always be at the forefront when designing certification schemes. If a scheme pursues additional objectives – e.g. industrial or geopolitical objectives –, the pursuit of these objectives should not under any circumstances conflict with the primary objective.[264] In addition, ENISA should only be allowed to take these other objectives into account in a scheme if it has received a mandate from the legislator to do so. This means that these objectives should already be enshrined in the CSA at Level 1. The scope for ENISA or the Commission to act at Level 2, i.e. by means of an implementing or delegated act, should be strictly limited in this regard. If these additional objectives are important to the legislators, consideration should also be given to placing them in a hierarchy and establishing guidelines on how ENISA and the Commission should proceed in the event of any conflicts of objectives. Finally, clear criteria are needed to determine which aspects ENISA should consider when designing a scheme and those to which it should not attach any importance.
- Clear deadlines for the development of a cybersecurity certification scheme: The CSA does not currently make the stakeholders involved in the development of a cybersecurity certification scheme subject to any deadlines regarding the duration of the development process. A lot of time can therefore pass without any result between the issue of a mandate to ENISA by the Commission and the adoption of a new scheme (cf. the still ongoing process of developing an EUCS). However, the lack of such deadlines and the associated delay in establishing new schemes not only weakens the credibility of cybersecurity certification of ICT products, services and processes per se, but also ensures a lack of legal and planning certainty for cloud providers and users. When revising the CSA, clear deadlines for the establishment of new schemes – for example, a maximum of two years – should therefore be established. The length of procedures for consulting the various stakeholders could also be specified at Level 1 in order to outline and establish the path to developing a scheme even more precisely.
- Duty of transparency with regard to the current status of a scheme: In recent years, it has become apparent that it is very difficult for stakeholders and the general public to find out about the current status of individual schemes. New, adapted and revised versions of the drafts of individual schemes often only reach the public, if at all, via specialised media, while ENISA itself has only made sporadic attempts to proactively publish them. More transparency is urgently needed in this regard to ensure confidence in new schemes. This transparency should enable interested parties to comment on and scrutinise new or amended requirements, especially those that are considered non-technical. The additional transparency should without fail go beyond the consultation

[263] EU Commission (2025c), Call for Evidence for an impact assessment, The revision of the Cybersecurity Act, Ref. Ares(2025)2970891, 11 April 2025, See here.

[264] This could be modelled on an approach used in the EU Regulation on the establishment of a framework to facilitate sustainable investment ("green taxonomy"). Accordingly, a scheme must make a "significant contribution to the realisation of the objective of strengthening cybersecurity. If other objectives are – additionally – pursued, these must not "significantly harm" the objective of cybersecurity ("do no significant harm", DNSH concept") [similarly, see Art. 3 of Regulation (EU) 2020/852 on the establishment of a framework to facilitate sustainable investment and amending Regulation (EU) 2019/2088].

process already prescribed in the CSA by ENISA.[265] The new transparency requirements introduced as part of the amending Regulation in relation to managed security services represent a good first step in this direction but are not yet sufficient.[266,267]

- Delegated act instead of implementing act: The Commission should define future EU certification schemes (i.e. also a future EUCS) by means of delegated acts (Art. 290 TFEU) instead of implementing acts (Art. 291 TFEU). This would also strengthen their democratic legitimacy. At the same time, the EU legislator should regulate all essential aspects itself at Level 1, i.e. all those requirements that implement the fundamental orientation of EU policy[268], including, for example, whether – and if so which – sovereignty requirements must be taken into account when designing an EUCS at Level 2.
- Check the confidence of potential users of certified ICT products, services or processes in new EU schemes: A key and important objective of the EU cybersecurity certification framework is to strengthen trust in ICT products, services and processes.[269] However, trust can only be increased if the finalised EU cybersecurity certification schemes and the certificates based thereon are considered credible and perceived as trustworthy by potential users. If this is not the case, they are ultimately worthless. It therefore seems sensible to specifically consult the potential users of the ICT products, services or processes that are to be certified under the scheme before adopting a new scheme. Both users who are free to use the certified products, services or processes and those who are (possibly in the future) obliged to do so should be surveyed. When gathering opinions on a finalised scheme, the focus should be on whether a scheme promotes trust, whether it is actually considered effective, useful and necessary and whether it ultimately meets with broad acceptance.
- Early involvement of EU legislators: Switching from implementing acts to delegated acts, as proposed above, already involves a strengthening of democratic legitimisation. However, in order to further prevent political conflicts over the design of cybersecurity certification schemes, it seems necessary to involve political decision-makers in the development of the schemes at an early stage, but also to give them clear limits on "interference" in the primarily technical design process.
- Retain the voluntary approach, in principle: Under the CSA, recourse to European cybersecurity certification is generally voluntary.[270] This principle should also be upheld in the revision of the legislative act in order to avoid creating excessive new barriers to market entry or slowing down innovation. Even without mandatory EU certification, both sides of the market – cloud providers and cloud users – have the option of deciding in favour of or against the use of an EU certificate. If a certificate is an important quality feature for potential cloud users, it will also prevail on the

[265] When developing a possible scheme, ENISA must consult all relevant stakeholders through a "formal, open, transparent and inclusive consultation process" [see Art. 49 (3) Regulation (EU) 2019/881.

[266] Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services.

[267] In future, the Commission will have to provide public information when it requests ENISA to develop a cybersecurity certification scheme or review an existing scheme. The European Parliament and the Council can request the Commission and ENISA to provide information on the draft scheme on a quarterly basis during the preparation of a scheme. With the agreement of the Commission, ENISA can make relevant parts of a draft scheme available to the European Parliament and the Council, subject to the necessary confidentiality and, where appropriate, in a restricted form [new Art. 49a Regulation (EU) 2024/...].

[268] CJEU, Judgement of 27 October 1992, Case C-240/90, Germany v. Commission, ECLI:EU:C:1992:408, para. 37. See section 3.5.1 above on this.

[269] Recitals 65 and 69 Regulation (EU) 2019/881.

[270] Recital 91 and Art. 56 (2) Regulation (EU) 2019/881.

market and cloud providers will (have to) react accordingly in order to survive on the market – and vice versa.

- Central cornerstones for cloud cybersecurity certification schemes: The requirements set out in a cloud cybersecurity certification scheme should be risk-based and fact-driven and reflect the outcome of an objective risk assessment that considers the likelihood and consequences of undesirable potential cybersecurity incidents. Furthermore, the requirements must be proportionate. This is because every regulatory requirement for the use of – only certain – cloud services represents a restriction of entrepreneurial freedom and therefore requires justification. The additional benefit generated by the use of a certificate must in any event be proportionate to the (anticipated) additional costs incurred. In principle, a cloud scheme should also be designed to be as competition-neutral as possible. Any regulatory requirement for (still) permissible cloud services should not favour or disadvantage, and still less completely exclude any provider per se ex ante. Every cloud provider should be able to obtain certifications for the cloud services they offer, regardless of the level of assurance.

4.3 Revision of the NIS 2 Directive

The Directive on measures for a high common level of cybersecurity across the Union [Directive (EU) 2022/2555, NIS 2 Directive] is regarded as the first horizontal legislation on cybersecurity at EU level. It is currently being transposed – in many cases late – into national law by the Member States.[271] The Directive requires Member States to ensure that, in particular, "essential" and "important" domestic entities must take "appropriate and proportionate technical, operational and organisational measures" to enable them to manage the risks to the security of their network and information systems. The measures are also intended to "prevent or minimise the impact of security incidents on the recipients of their services and on other services".[272] The measures should also include steps to safeguard the "security of the supply chain" and therefore also "security-related" aspects with regard to the relationship between an entity and its direct suppliers or service providers. In doing so, the entities must also focus on the vulnerabilities of these suppliers and their cybersecurity practices.[273,274]

The NIS 2 Directive does not currently restrict the choice of supplier or service provider a priori. Essential and important entities are therefore basically free to decide whether and, if so, which cloud services they want to use – as part of the risk management measures they have to pursue. However, Member States have the option of obliging them to use only specific ICT products, services – including cloud services – or processes that are certified according to an EU cybersecurity certification scheme.

[271] On 28. 11. 2024, the EU Commission decided to initiate infringement proceedings against a total of 23 Member States (including Germany, Spain, France, the Netherlands, Austria and Poland) who had not fully implemented the NIS 2 Directive by this date (see here).

[272] Art. 21 (1) Directive (EU) 2022/2555.

[273] Art. 21 (2) and (3), Directive (EU) 2022/2555.

[274] This includes in particular the definition of a "supply chain security concept" which has to contain "criteria for selecting and using suppliers and service providers", including their cybersecurity practices, their ability to meet cybersecurity specifications set by the organisation, the overall quality and resilience of ICT products and services, and the entity's ability to diversify its sources of supply and limit dependencies on specific vendors. Furthermore, contracts with suppliers and service providers must – where appropriate – contain cybersecurity requirements in the form of performance agreements. For example, security requirements also have to be defined which must apply to the ICT services or ICT products to be purchased and which must be guaranteed by the suppliers [see Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down detailed rules for the implementation of Directive (EU) 2022/2555 [...]].

Only such certification would then provide proof that the entity is complying with the prescribed risk management measures.[275]

However, this regulatory approach has a number of weaknesses that should be addressed as part of a revision of the NIS 2 Directive:

1. More standardised identification of essential and important private entities

Firstly, the criteria and procedures used to identify essential and important entities should be revised by the Member States. The revision of the NIS 2 Directive in 2022 did succeed in limiting the Member States' room for manoeuvre in this regard, thereby limiting regulatory arbitrage and distortions of competition. However, identification should not only be based on the size of the entity – which is currently the central criterion – but also on other factors, such as the entity's number of customers or users. The actual size of an entity does not necessarily or solely indicate a higher cybersecurity risk. The scope of the NIS 2 Directive should also only ever cover those entities that are central to the functioning of an economy. In any case, the definition of the entities that are to fall within the scope of the Directive should be as standardised as possible in order to prevent individual relevant entities in the Member States from evading the security requirements of the Directive or to avoid distortions of competition. Such a standardised definition would be particularly important for those companies or sectors that are in cross-border competition with each other (e.g. banks, energy companies, companies in the transport sector). A standardised approach would ensure that the same requirements apply to all entities that are subject to comparable cybersecurity risks, particularly with regard to requirements for selecting suitable cloud services.

2. Examination of an obligation for certain essential and important entities to exclusively use certified cloud services

The question is whether individual (groups of) non-governmental entities falling within the scope of the NIS 2 Directive should be explicitly obliged to use only cloud services that are certified in accordance with a future EUCS.[276] The Directive already allows Member States to adopt such an obligation. However, this clause harbours the risk that a variety of approaches will be taken, leading to regulatory fragmentation and thus a weakening of the digital single market. It would in principle, therefore, seem appropriate to consider such an obligation only for those private entities operating in highly sensitive fields of activity, although defining these would primarily be a (socio-)political decision. Furthermore, such an obligation should only apply to those non-governmental entities which are likely to cause major cybersecurity risks to third parties if the entities themselves fail to use cloud services with a high degree of security, i.e. in cases where entities fail to take potential damage to third parties into account in their decision-making process when choosing a cloud service (lack of internalisation of negative external effects). In addition, such an obligation may be of particular importance where the relevant entities are or could be active not only nationally but also across borders (see above).

3. Reduce fragmentation of scope regarding public administrations and review an obligation to use certified cloud services for selected public administration entities

The EU should also consider introducing an obligation to exclusively use certified cloud services for specific and narrowly defined public administrations if they wish to process and store particularly

[275] Art. 24, Directive (EU) 2022/2555.

[276] This of course presupposes the prior acceptance of the EUCS and should not be taken to mean that the entities concerned would even have to use cloud services.

sensitive data in the cloud.[277] In this regard, it would first make sense to revise and harmonise the scope of the NIS 2 Directive with regard to such administrations. Currently, public administration entities fall within the scope if – regardless of their size – they are entities of central government[278], or at regional level but in the latter case only if they provide services "the disruption of which could have a significant impact on critical societal or economic activities".[279]

On the other hand, Member States have the option of applying the NIS 2 Directive to public administration entities at local level.[280] If a public administration entity carries out activities in the areas of national security, public security, defence or law enforcement, it is generally excluded from the scope.[281]

The resulting "patchwork" in relation to the applicability of the NIS 2 Directive to public entities should be resolved or further limited. For example, the level – central, regional or local – should not be the primary deciding factor for inclusion in the scope of the legislation. This should in fact be the social and economic impact that a failure or security breach at the relevant public administration would have for the EU Member State in question, as well as EU-wide.[282] The extent to which a public administration or a certain category of public administration is relevant to the internal market, i.e. the extent to which it shares or exchanges data and information with administrations in other EU Member States as part of its activities, for example, should also play an important role. If this patchwork were to be ironed out, standardised criteria for the (non-)inclusion of public administrations defined and, in particular, greater attention given to administrations below the level of central government, much would already have been achieved towards strengthening cybersecurity in the EU.

Standardising the scope of the NIS 2 Directive with regard to public administration entities could then form the basis for more precisely stipulating a priori that certain administrations, which would then be subject to the NIS 2 Directive, may in future only use cloud services that are certified in accordance with an EU cybersecurity certification scheme.[283] For these steps to be taken, an adaptation of Article 24 of the NIS 2 Directive should be considered.[284] The option that Member States "may" require entities to use cloud services certified under the EU cybersecurity certification scheme could be maintained for less critical environments. At the same time, consideration should be given to turning the option ("may") into an obligation ("must") for public entities that manage, process and store (highly) sensitive data or where there is a regular (cross-border) exchange with other public entities (i.e. in particular administrations with relevance for the single market).[285] And, at the same time, as part of an

[277] Nevertheless, the public organisations in question should always have the option of doing without cloud services altogether.
[278] Art. 2 (2) (f) (i) NIS-2 Directive.
[279] Art. 2 (2) (f) (ii) NIS-2 Directive.
[280] Art. 2 (5) (a) NIS-2 Directive.
[281] Art. 2 (7) NIS-2 Directive.
[282] However, the existing exemption for public administration entities carrying out activities in the areas of national security, public security, defence or law enforcement should be maintained. Taking these organisations into account would probably encroach too far on the sovereign rights of the individual Member States.
[283] This should not be understood to mean that public administration organisations must generally use cloud services. They should also be allowed to dispense with their use entirely in the future.
[284] In particular, Article 24 provides that "Member States […] may require essential and important entities to use particular ICT products, services and processes developed by the essential or important entity or procured from third parties that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881 […]".
[285] Public administration organisations are neither profit-oriented nor do they compete with other administrations. However, a commitment to the use of harmonised EU certification standards could promote the exchange of data between administrations and between administrations and users of public services – citizens and businesses – and have a confidence-building effect.

amendment to Article 24, assurance levels could then be specified, which would remain open to the obligated public entities in the future. This could boost the development of cyber-secure markets for cloud services in the EU, enable economies of scale on the part of interested cloud service providers and thus also contribute to reducing the costs of using secure cloud services. The approach outlined here could therefore be a possible first blueprint for Henna Virkkunen to implement the proposal outlined in her so-called "Mission Letter" for the creation of an "EU-wide cloud policy for public entities".[286]

4. Limiting the EU Commission's scope to oblige organisations to use certified cloud services

Currently, under the NIS 2 Directive, the Commission can also use delegated acts to define "categories" of essential and important entities that (a) may only use certain certified ICT products, services and processes, or (b) must obtain a certificate from an EU cybersecurity certification scheme.[287] The Commission's power to make such determinations independently should be reconsidered. In the interests of strengthening democratic legitimacy, such decisions should not be taken by the Commission via delegated acts, but by the EU legislator – the Council and the European Parliament – (at Level 1). This is particularly true since the leeway granted to the Commission in this respect by the NIS 2 Directive appears to be excessive. Thus, the Commission can always take action if an inadequate level of cybersecurity has been identified. This wording raises various questions, however, notably as to when a cybersecurity level should be considered "inadequate" and who actually has to make the determination. This lack of clarity should also be addressed as part of a targeted revision of the NIS 2 Directive. The first step would be for the EU legislator to define the categories of essential and important entities at Level 1. At the same time, the Commission should review the Directive every two to three years and determine whether new categories of entities should be added, or existing categories removed. If the Commission reaches such a judgement, it should submit a reasoned legislative proposal for the targeted adaptation of the Directive. The EU legislator should then decide whether the envisaged amendment is necessary and initiate corresponding changes to the NIS 2 Directive at Level 1.

4.4 Short-term ways out of the debate on sovereignty requirements ("bridging options")

As already mentioned, the EU Commission, ENISA, the Member States and other stakeholders involved in the development of a cloud cybersecurity certification scheme (EUCS) have not yet been able to agree on whether it should contain "sovereignty requirements" at all and, if so, how these should be structured. There are currently no signs of a compromise – a "European common ground" – which is why the actual centralised adoption of such a scheme is being continually put off to a later date. As already mentioned, one solution would be to initially adopt an EUCS without strict sovereignty requirements.

Bridging Option 1: The EU Commission, in cooperation with ENISA, the Member States and relevant stakeholders, could develop standardised sovereignty requirements in the form of EU guidelines, possibly including an EU label, which would be non-binding and not part of the EUCS, but could provide important guidance for (potential) users of cloud services for whom cloud sovereignty issues are or should be important. Cloud service providers with an interest in offering "sovereign clouds" in line with the EU guidelines could then actively advertise that they fulfil or wish to fulfil the sovereignty

[286] EU Commission (2024b).
[287] See Art. 24 (2) NIS Directive.

requirements set out in the EU guidelines. This could also include the introduction of a corresponding label requiring prior verification by an external body as to whether the cloud service provider fulfils the corresponding requirements.[288] Although, due to their voluntary nature, cloud providers would not necessarily have to fulfil sovereignty requirements contained in guidelines but could also use their own sovereignty requirements and/or sovereignty requirements that deviate from the EU guidelines (which would admittedly leave the internal market fragmented), this would simultaneously open up competition for the most "credible and trustworthy" sovereignty requirements. If potential cloud users consider the EU criteria to be credible and/or trustworthy, these will prevail on the market and thus establish an EU standard. The situation would be de facto, if not de jure, similar to that under an EUCS with sovereignty requirements. However, if users do not consider the EU criteria to be credible and trustworthy, other – e.g. national, company-specific or industry-specific – criteria will assert themselves in competition, which in turn would provide an opportunity to revise the criteria set out in the EU guidelines if necessary. In view of current political developments, notably the “Trump effect”, companies, public authorities and private users appear to be increasingly looking for alternatives to US service providers, even without sovereignty criteria included in a EUCS.[289] However, it is not yet clear whether these movements will be a long-term trend.[290]

Bridging Option 2: As an alternative or in addition to Bridging Option 1, the EU Commission could also draw up guidelines on how or in what form cloud service providers should inform potential cloud service users that their cloud services fulfil certain sovereignty requirements ("transparency instrument"). In these guidelines, it could provide specific guidance on the various elements of sovereignty requirements – e.g. data residency requirements, ensuring immunity from non-EU law or corporate governance – and provide examples of best practice. On the one hand, such guidelines could serve as a standard for how cloud service providers may or should present or market their services as "sovereign" and, on the other hand, serve as an aid for (potential) users of cloud services when selecting supposedly "sovereign" clouds.

4.5 Long-term options for action regarding sovereignty requirements

If the EU guidelines, which are intended as bridging options, prove successful and gain a certain market penetration ("market acceptance"), the next step could be to examine whether the "successful" requirements set out in the guidelines could be integrated into a revised cloud certification scheme. Such integration should take place either by

- the EU legislator itself formulating the sovereignty requirements to be included in a cloud certification scheme at Level 1 – i.e. as part of a legislative project – as well as the (sensitive) cases in which these are to be applied to certain cloud users, or
- the EU legislator explicitly mandating the Commission at Level 1 and authorising it to take sovereignty requirements into account when developing a cloud certification scheme – in cooperation with ENISA and by means of delegated acts[291]. However, it should be clearly specified at Level 1 which categories of sovereignty requirements – e.g. immunity from non-EU law – may be included in the EU scheme and which may not.

[288] As the step outlined above is only intended as a bridging option, the use of a label and the external audit could also be omitted for the time being if necessary. The decision should depend on how long the bridging phase is expected to last.
[289] Ernst, N., (2025) More Interest in European Cloud Providers due to the "Trump-Effekt", see here.
[290] Donath, A. (2025), EU-Tech-Firmen erleben Aufschwung durch US-Handelspolitik, see here.
[291] Due to stronger democratic feedback, delegated acts are preferable to implementing acts.

Regardless of which option is chosen, the proposed changes could be integrated into a revised CSA.

4.6 Harmonised EU policy on public tendering for cyber-secure cloud services

In summer 2024, in her political guidelines for the European Commission 2024-2029[292], Commission President von der Leyen announced that she wanted to revise the "Directive on the award of public contracts (Directive 2014/24/EU[293])" in the new legislative period in order to "give preference to European products when awarding public contracts in certain strategic sectors"[294].[295] In his competitiveness report published in September 2024[296], Mario Draghi also proposed the development of a "uniform EU-wide policy for the procurement of cloud services by public administrations" which also aims to include "data residency requirements".[297,298] Accordingly, the new EU Commissioner Henna Virkkunen was also instructed in her aforementioned mission letter to develop a "single EU-wide cloud policy for public administrations and public procurement".[299] Initial indications suggest that such an EU-wide cloud policy will be accompanied by standardised procurement specifications[300] and a curated "EU marketplace for secure and innovative cloud services"[301,302], and will be aimed at

- further harmonising the requirements faced by public administrations in different EU Member States when requesting cloud services from different providers, and
- making it easier for public administrations to identify the cloud services that best meet their security and sovereignty preferences.

In its recently published communication on a "Competitiveness Compass for the EU", the Commission announced that it will propose a "European preference in public procurement for strategic sectors and technologies" as part of a forthcoming review of the Public Procurement Directives. This is to reinforce technological security to safeguard Europe's own capacities.[303] This announcement was specified in the Commission's ambitious communication on a "Clean Industrial Deal" calling for non-price related criteria in public procurement, including on resilience aspects as well as "EU content requirements in

---

[292] EU Commission (2024d), Europe's Choice, Political guidelines for the next European Commission 2024-2029, Ursula von der Leyen, candidate for President of the European Commission, 18 July 2024.

[293] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.

[294] EU Commission (2024d), p. 14.

[295] On 13 December 2024, the Commission also launched a Consultation on the evaluation of the Public Procurement Directives. It aims to obtain opinions on whether Directives 2014/23/EU, 2014/24/EU and 2014/25/EU have proved their worth. The Commission wants to examine whether the Directives are still suitable, appropriate and fit for purpose in order to achieve the EU's political objectives.

[296] EU Commission (2024a).

[297] The aim is to harmonise public procurement in all Member States in order to standardise tenders and facilitate and promote cooperation between EU companies. However, Draghi argued for exceptions in nationally sensitive areas (e.g. defence, home affairs and justice) [EU Commission (2024a), p. 84].

[298] EU Commission (2024a), p. 84.

[299] EU Commission (2024b).

[300] Interestingly, the EU Commission already announced such a step in February 2020 in its EU data strategy (see cep**PolicyBrief**). This states that it wants to "facilitate the development of common European standards and requirements for the award of public contracts for data processing services" and also refers to similar steps in the USA ("FedRAMP" programme for the award of public contracts) [see EU Commission (2020a)].

[301] This proposal was also already part of the EU data strategy of February 2020 (see cep**PolicyBrief**). In it, the Commission stated that it wanted to promote an EU marketplace for cloud services for users from the private and public sectors, which should support the selection of cloud services that meet certain requirements in terms of "data protection, security, data portability, energy efficiency and market practice" and, among other things, "facilitate the procurement of alternative solutions for the public sector" [see EU Commission (2020a)].

[302] European Parliament (2024), Questionnaire to the Commissioner-designate, Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy.

[303] EU Commission (2025d), COM(2025) 30, Communication, A Competitiveness Compass for the EU, 29 January 2025.

line with the Union's international legal commitments". As part of the revision of the Public Procurement Framework, scheduled for the Q4 2026, beyond sustainability, both "resilience and European preference criteria" shall be included in EU public procurement, at least for strategic sectors.[304]

Public procurement is indeed a key economic policy instrument and could be an important lever for steering the European economy in politically desirable directions. This is clear from the fact that spending on public procurement accounts for around 14% of the EU's gross domestic product (GDP) each year.[305,306]

In 2014, as part of the revision of the Public Procurement Directive[307], EU legislators agreed to make greater use of public procurement as a "strategic instrument" to better meet important social challenges facing the EU.[308] In particular, the reform aimed to ensure that contracting authorities make strategic use of procurement procedures for works, goods and services. Instead of focusing solely on price as the most important criterion, they should take greater account of ecological and social objectives and thus use procurement to drive innovation. This would also contribute to "increasing the efficiency and quality of public services".[309] At the same time, the principle that the consideration of such strategic objectives must not "artificially narrow competition" should continue to apply which means that a procurement procedure must not be designed with the intention of "unduly favouring or disadvantaging certain economic operators".[310]

The idea now being promoted by the Commission to give preference to products from the EU when awarding public contracts in certain strategic sectors – including the cloud computing sector – is aimed at further strengthening the strategic component in public procurement[311] and at the same time artificially restricting competition – contrary to the current legal situation – by discriminating against non-EU products.

Box 3

1) "Net Zero Industry Act": Criteria for environmental sustainability and cybersecurity in public procurement with regard to net zero technologies

On 13 June 2024, Regulation (EU) 2024/1735 establishing a framework for measures for strengthening Europe's net-zero technology manufacturing ecosystem ("Net Zero Industry Act") entered into force. The Regulation has largely been in force since the end of June 2024.

The central aim of the "Net Zero Industry Act" is to ensure that the EU has access to a secure and sustainable supply of so-called net-zero technologies.[312] A key measure to achieve this goal is the promotion of "demand

[304] EU Commission (2025e), COM(2025) 85, Communication, The Clean Industrial Deal: A joint roadmap for competitiveness and decarbonisation, 26 February 2026.
[305] EU Commission (2017), COM(2017) 572, Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Making public procurement work in and for Europe, 3 October 2017.
[306] EU Commission (2024d), Europe's Choice, Political guidelines for the next European Commission 2024-2029, Ursula von der Leyen, candidate for President of the European Commission, 18 July 2024.
[307] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC.
[308] EU Commission (2017), p. 3.
[309] Recitals 47, 93 and 97 Directive 2014/24/EU.
[310] Art. 18, Directive 2014/24/EU.
[311] As part of the "Net Zero Industry Act", EU legislators have already agreed on such steps with regard to net zero technologies. In October 2024, the Federal Ministry for Economic Affairs and Climate Protection (BMWK) also presented proposals for a more strategic approach to public procurement as part of a "procurement transformation package". They were adopted in revised form by the German Federal Cabinet at the end of November 2024 (see Box 3).
[312] Art. 1 (1) Regulation (EU) 2024/1735.

for sustainable and resilient net-zero technologies through public procurement procedures".[313] In particular, the Regulation stipulates that contracting authorities must apply **"minimum mandatory requirements regarding environmental sustainability"** when awarding public contracts if net-zero technologies are part of the contracts or if construction contracts or construction concessions include net-zero technologies.[314] The Commission must adopt an implementing act by the end of March 2025 to define the minimum requirements mentioned.[315]

In addition, contracting authorities must apply at least one of several "conditions, requirements or contractual obligations" to works contracts and works concessions involving net zero technologies. This includes the requirement that the contractor must demonstrate **compliance with the applicable cybersecurity requirements** set out in "a cyber resilience regulation". Where appropriate and available, this can also be done **via a relevant European cybersecurity certification system**.[316]

The "Net Zero Industry Act" also provides for the introduction of **"resilience criteria"**. This is reflected, for example, in requirements that no more than 50% of the EU supply of a net-zero technology may come from a single third country.[317]

---

2) "Procurement transformation package" of the German Federal Ministry for Economic Affairs and Climate Action (BMWK): Criteria for social and ecological procurement and the potential exclusion of bidders from third countries

On 18 October 2024, the Federal Ministry for Economic Affairs and Climate Action presented draft bills for the reform of public procurement law ("Public Procurement Transformation package"). The package aims to simplify, digitalise and accelerate public procurement procedures, to make public procurement economically, socially, ecologically and innovatively oriented and to strengthen the binding nature of the procedures.[318] The BMWK wanted to[319,320]

- make public procurement more sustainable. To this end, the state should **consider socio-ecological criteria as a rule in future** and thus provide "leverage for a transformative economy" and contribute to the creation of green lead markets. To achieve this, for example, the discretion of contracting authorities with regard to the consideration of social and environmental criteria is to be limited (new Section 120a GWB), and
- create the possibility that **applicants and bidders from certain third countries[321] can be excluded** from certain public contracts in order to increase the security of Germany. This involves contracts in the areas of (a) critical infrastructure within the meaning of the BSI Act and (b) defence and security (new Section 112a GWB). Whether such an exclusion takes place shall be at the discretion of the contracting authority.[322]

[313] Art. 1 (2) Regulation (EU) 2024/1735.
[314] Art. 25 (1) Regulation (EU) 2024/1735.
[315] Art. 25 (5) Regulation (EU) 2024/1735.
[316] Art. 25 (3) (b) Regulation (EU) 2024/1735.
[317] Recital 57 and Art. 25 (7) Regulation (EU) 2024/1735.
[318] See BMWK overview of the procurement transformation package.
[319] Bundesministerium für Wirtschaft und Klimaschutz (2024), Referentenentwurf des Bundesministeriums für Wirtschaft und Klimaschutz, Allgemeine Verwaltungsvorschrift zur Berücksichtigung sozialer und umweltbezogener Kriterien bei der Vergabe öffentlicher Aufträge, 18 October 2024.
[320] Bundesministerium für Wirtschaft und Klimaschutz (2024), Referentenentwurf des Bundesministeriums für Wirtschaft und Klimaschutz, Entwurf eines Gesetzes zur Transformation des Vergaberechts (Vergaberechtstransformationsgesetz), 18 October 2024.
[321] This refers to third countries that do not have privileged access to the EU's public procurement market under international law.
[322] See also W. Witte (2024) Vergabetransformation im Überblick: Das plant die Ampel, 14 October 2024, available here.

On 27 November 2024, the German Federal Cabinet passed the draft bill for the "Public Procurement Law Transformation Act".[323] This **no longer contains the passage on excluding applicants and bidders from certain third countries.** This change was probably due to the CJEU ruling of 22 October 2024, in which the Court of Justice ruled that the regulation of access to procurement procedures in the Member States for economic operators from third countries falls within the exclusive competence of the EU.[324,325]

Interestingly, however, it has been shown that the use of public procurement for strategic purposes has not exactly enjoyed a resounding success. As early as 2017, the Commission itself emphasised that the lowest price continues to be the "sole award criterion" in 55% of tenders and that in practice environmental, social and innovation-related aspects are rarely taken into account.[326] Recently, the European Court of Auditors also emphasised that the 2014 reforms had "no demonstrable effect" and that strategic aspects were "rarely considered" in public procurement procedures. Thus, "the share of contracts awarded in favour of lowest bid still accounts for the bulk of all awards in all member states" and competition decreased over the period 2011-2021.[327] In its reply to the Court of Auditors, the Commission recognises that "the increasing complexity of procurement" and more strategic procurement mean that procurement procedures are becoming more complex and lengthy, the cost of tendering is rising and participation in tenders is decreasing.[328]

If, in the new legislative period, the Commission now proposes to further strengthen the strategic flank of public procurement to secure the EU's digital sovereignty[329] – for example by favouring European cloud services that also promise to fulfil certain cybersecurity requirements (ex- or inclusive sovereignty requirements) – it should not ignore the experience gained from the application of the existing EU procurement directives mentioned above. Based on this experience, it seems that, in practice, Member States are unlikely to give a lot of attention to "additional" strategic aspects, especially in view of tight budgets. However, if this is the case, the consideration of the strategic factors becomes superfluous a priori. It must also be borne in mind that such consideration – if applied by the Member States – could lead to a further reduction in the number of possible bidders for public contracts and thus reduce competition beyond the already low level. This in turn would make public procurement more expensive and thus poses the risk of wasting precious taxpayers' money. Finally, three other aspects must not be ignored: Firstly, adding to the criteria to be taken into account when awarding contracts will add to a growing bureaucratic burden, both for the bidders, who have to fulfil the additional criteria, and for the contracting authorities, who have to check whether these criteria are actually fulfilled.[330] Secondly, having to consider additional aspects that go beyond price, environmental, social and innovation-related factors risks creating further trade-offs that are difficult to resolve (the low price of a cloud solution v. cloud service with EU data localisation, or access to innovative,

[323] Bundesregierung (2024), Transformation des Vergaberechts, Einfacher und schneller vergeben Aufträge, 27.11.2024, available here.
[324] CJEU (2024), Case C-652/22 (Kolin Inşaat Turizm Sanayi ve Ticaret).
[325] See also Rosenkötter, A. (2024), Kein geschützter Marktzugang für Bieter aus Drittstaaten – jetzt alles geklärt?, CJEU, Judgement of 22.10.2024 – C-652/22 – "Kolin", available here.
[326] EU Commission (2017).
[327] European Court of Auditors (2023), Special Report on Public Procurement in the EU: Less competition for contracts awarded for works, goods and services in the period 2011-2021, 4 December 2023.
[328] EU Commission (2024e), Replies of the European Commission to the European Court of Auditors' special report, Public procurement in the EU, Less competition for contracts awarded for works, goods and services in the 10 years up to 2021.
[329] Surveys actually show an increased interest, at least among public administrations in Germany, (a) in the implementation of cloud solutions in the next few years per se (66%) and (b) in the importance of digital sovereignty issues (95%) (for more information, see here).
[330] This would ultimately also thwart the new EU Commission's goal for the current legislative period of reducing administrative burdens and simplifying EU law.

environmentally beneficial cloud services v. a cloud solution that is "immune" to non-EU law). And thirdly, there is a risk of overloading the tendering process, which could further impede the award of contracts.

In view of these practical experiences, uncertainties and potentially undesirable side effects of a more "strategic" agenda for public procurement aimed at digital sovereignty, the path envisaged should only be pursued to a limited extent. In particular, it should be limited to those areas where the security interests of the EU or the Member States – for example with regard to data sovereignty – are given greater weight[331] than other factors such as the price or innovative features of a cloud service. In all other cases, although public procurement can be a crucial lever for both the creation and development of (new) markets – in terms of lead markets for "sovereign" clouds from the EU – ultimately, the state-driven establishment of such "lead markets", which goes hand in hand with favouring certain companies and disadvantaging others, contradicts the free market economy, as the state is aiming to predetermine certain market outcomes ex ante. The lever of public procurement should therefore only be used to a limited extent and restricted to narrowly defined areas.

Finally, the Commission envisages the establishment of curated "EU marketplaces for secure and innovative cloud services" to make it easier for public administration organisations to identify the cloud services that meet their security and sovereignty preferences.[332,333] Such marketplaces can be a useful transparency tool, make it easier for organisations to make decisions, reduce the practical workload of potential government contractors and contribute to a reduction in transaction costs. They can also stimulate competition, as they make it easier for users of cloud services to compare different offers. However, the question arises as to whether such marketplaces could not be organised, established and operated by the private sector. If there is a particular need for information on the security features of cloud services on the part of potential public-sector cloud consumers, cloud providers are likely to have a vested interest in providing this information, whether on privately organised digital purchasing platforms or otherwise. Intervention by the Commission or the EU legislator would then be unnecessary. Any private sector initiatives could, where necessary, be flanked by non-binding guidelines or handouts outlining possible elements of such marketplaces. Private marketplace operators should also be obliged to disclose the criteria for the inclusion or non-inclusion of individual cloud providers on their platform. However, any action at EU level should not undermine competition for the best online marketplaces for – cyber-secure/innovative – cloud services for public administrations. If the EU Commission nevertheless sticks to the idea of such marketplaces being developed by the public sector, firstly it should not replace the private marketplaces but simply attempt to supplement them. Secondly, it should build on existing best practices in the Member States. It remains to be critically examined whether state marketplaces are necessary at both levels – i.e. at both Member State and EU level. In terms of strengthening the internal market and developing competitive and cross-border procurement markets, a restriction to EU marketplaces would be preferable and help to conserve the state's already tight financial resources.

[331] This could include, for example, intelligence service information, tax data, health data or defence-related information.

[332] At present, procurement via online marketplaces is generally not possible, as this method does not fit into the usual structure of procurement procedures. One exception is the so-called "direct order", in which a company is commissioned without a procurement procedure being carried out. For more details see here.

[333] European Parliament (2024), Questionnaire to the Commissioner-designate, Henna Virkkunen, Executive Vice-President for Tech Sovereignty, Security and Democracy.

5 Further developments affecting the debate on the cybersecurity of cloud services

5.1 Data access for effective law enforcement and its potential to undermine cybersecurity

On 1 April 2025, the Commission has published "ProtectEU", the new European Internal Security Strategy,[334] which sets out the main internal security policies for the years ahead. The strategy aims to provide a comprehensive response to man-made threats to the EU's internal security such as hybrid threats, organised crime and terrorism.[335] It is guided by three principles: first, by a whole-of-society-approach for actions under the strategy, involving all citizens and stakeholders; second, the need to mainstream security considerations across all EU legislation, policies and programmes, and third, the intention to boost serious investment in security by the EU, its Member States and the private sector. Inter alia, the Commission intends to equip the EU with "new ways of sharing and combining information", provide "a regular EU internal security threat analysis" and intends to propose stronger rules to tackle organised crime. Beyond this, the Commission wants the EU to develop new tools for law enforcement, such as a revamped Europol, and better means of coordinating and ensuring secure data exchange as well as "lawful access to data". The reason for the latter is that for years, police forces and intelligence services have been complaining about a scenario according to which the increasing end-to-end encryption of communication – and messenger services in particular – threatens to make investigators blind and deaf. Police forces and intelligence services call this phenomenon "going dark".

The Commission should make sure that its plans to harmonize and strengthen law enforcement and prevent police investigations from "going dark" will not – in addition to the risk of generally compromising the security of communications of millions of users – create systemic risks to cybersecurity and the security of data storage. Insofar, the EU's various plans might contradict each other in this respect. On the one hand, the Commission refers in its new Internal Security Strategy to the persistent nature of malicious cyber activity and to the range of laws adopted by the EU to improve the level of cybersecurity in recent years, and expresses its willingness to develop further measures to ensure cybersecure use of cloud services.[336] In particular, the Commission announces that it will take action to encourage critical entities to choose cloud services which offer an appropriate level of cybersecurity, taking into account also technical risks.[337] On the other hand, the Commission wants to develop new tools for law enforcement including better means of coordinating and ensuring a supposedly "lawful access to data".[338] In more detail, in order to follow up on the recommendations[339] of the High Level Group on Access to Data for Effective Law Enforcement, which has been established in 2023, the Commission announces that it will present, until end of June 2025, "a roadmap setting out the legal and practical measures it proposes to take lawful and effective access to data" and, inter alia, prepare a "technology roadmap on encryption, to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, safeguarding cybersecurity and

[334] EU Commission (2025b), COM(2025) 148, Communication on ProtectEU: a European Internal Security Strategy, 1 April 2025, p. 12 and 17, see here.
[335] EU Commission (2025b1), Q&A on ProtectEU – a new European Internal Security Strategy, see here.
[336] EU Commission (2025b), COM(2025) 148, Communication on ProtectEU: a European Internal Security Strategy, 1 April 2025, p. 12 and 17, see here.
[337] EU Commission (2025b), loc. cit, p. 13.
[338] EU Commission (2025b), loc. cit, p. 4.
[339] Recommendations of the High-level Group on Access to Data for Effective Law Enforcement (2024).

fundamental rights".[340] This could also entail "systematic cooperation" between law enforcement authorities and private parties, including service providers[341] – which ultimately could also encompass providers of cloud services. Such cooperation with law enforcement authorities could even become mandatory for service providers, given the statement of the High-Level Group that in case of non-cooperating providers, authorities will still need to resort to the use of vulnerabilities in "exceptional" cases (e.g., primarily criminal services such as EncroChat), and its demand to harmonize the relevant safeguards and possibly rules for the mutual admissibility of evidence.[342] However, introducing vulnerabilities (such as backdoors in encryption) is very delicate, as it could create systemic risks affecting millions of users (see **cepAdhoc**).[343] It is highly questionable whether the Commission's plan to ensure uncritical and "lawful" access to encrypted data will be realistic at all. Critics argue that there are no technical way to break the promise of end-to-end encryption without weakening the security of communications systems, as any backdoor intended for law enforcement can always be exploited by malicious actors.[344] In any case, solutions that provide for a systematic weakening of encryption must be avoided, as the ultimate price may be too high: in addition to clear legal risks, there is a threat of undermined user trust, weakened cybersecurity and a chilling effect on innovation and SME investment.[345]

5.2 Envisaged AI and Cloud Development Act

In April 2025, the EU Commission has launched a call for evidence for an impact assessment and a public consultation on computing capacity in connection with the envisaged EU Cloud and AI Development Act, planed for Q4 2025.[346] The EU aims to massively increase computational capacity in the EU ("at least triple the EU's data centre capacity in the next five to seven years")[347] and, at the same time, tackle "the lack of a competitive EU-based offer of cloud computing services at sufficient scale to serve highly critical use cases with particularly high security needs, as found in various economic sectors and the public sector".[348] Inter alia, the Commission wants to "ensure that a set of narrowly defined highly critical use cases can be operated using highly secure EU-based cloud capacity, while creating the conditions for the EU cloud industry to develop secure processing capacities to serve the needs of these highly critical use cases".[349] General questions in the public consultation include whether the participant has concerns about data security and about a too high influence of non-EU tech companies over data and digital infrastructures and whether the EU should prioritise EU cloud infrastructure and services. Beyond this, all participants are asked to share their views on potential policies to be adopted on cloud policy. However, there are also more focused questions depending on the stakeholder category of the respondent (e.g. business/public administrations/citizens) and further specifications (e.g.

[340] EU Commission (2025b), COM(2025) 148, loc.cit., p. 7.
[341] EU Commission (2025b), COM(2025) 148, loc.cit., p. 6.
[342] Recommendations of the High-level Group on Access to Data for Effective Law Enforcement (2024), p. 7, 13 et seq., 22 et seq.
[343] For in-depth coverage of this topic, see Hoffmann, A. / Küsters, A. / Eckhardt, P., Security and Trust: An Unsolvable Digital Dilemma? cepAdhoc No. 5/2025, 11 March 2025, p. 6 et seqq., available here.
[344] Joint letter calling for the EU digital security agenda to promote fundamental rights and support a safe digital ecosystem, 11 December 2024, see here.
[345] For in-depth coverage of this topic, see Hoffmann, A. / Küsters, A. / Eckhardt, P., Security and Trust: An Unsolvable Digital Dilemma? cepAdhoc No. 5/2025, 11 March 2025, available here.
[346] EU Commission, Call for Evidence for an Impact Assessment, Cloud and AI Development Act, 9 April 2025, Ref. Ares(2025)2878100 , available here. The public consultation are open for feedback until 4 June, 2025.
[347] EU Commission, Press Release, 9 April 2025, see here.
[348] EU Commission (2025f), Call for Evidence for an Impact Assessment, Cloud and AI Development Act, 9 April 2025, Ref. Ares(2025)2878100 , p. 1, available here.
[349] EU Commission (2025f), loc. cit, p. 2.

Cloud providers/AI Developers/Cloud Users). The results of the survey could thus also have an indirect significance for the debate on the certification of the cybersecurity of cloud services and/or the backing of certain sovereignty criteria. Depending on the outcome of this consultation, the EU could potentially conclude that "EU cloud infrastructure and services" should be prioritised, for instance in certain areas such as public sector procurement. It is still open whether such location and control requirement will play a decisive role and/or even be made a prerequisite for certification under a yet to be adopted EUCS; if this will be the case, such services could inherently meet a possible future sovereignty requirement of "EU-based" cloud services.

6 Conclusion

The second term of office of Commission President von der Leyen began on 1 December 2024 and the newly appointed College of Commissioners has started its work. While the new legislative period is all about strengthening the EU's competitiveness, the Commission also has a number of plans for future EU cloud policy, some of which are already set for 2025.[350] Since the representatives of the Commission, the EU Member States and ENISA have been unable to reach a compromise acceptable to all sides in recent years with regard to the EU scheme for certifying the cybersecurity of cloud services (EUCS), a new attempt to break the deadlock in a productive way is urgently needed. However, a different route should be taken from the one proposed by Sarah Knafo, a French MEP, recently stipulated in the ITRE-Committee in the European Parliament.[351] This cep**Input** has come up with some possible ways out of the impasse and options for action and put forward initial ideas for a future resilient EU cloud policy. Our proposals range from the need to dispel doubts about the rationale and advisability of sovereignty requirements as a basis for a credible EU cloud policy, to the compelling need to create a legal basis for the introduction of sovereignty criteria in an EU cybersecurity certification scheme by way of a legislative act (i.e. at Level 1) and the adaptation of relevant EU legislation such as the EU Cybersecurity Act, the NIS 2 Directive and the EU rules on public procurement. At the same time, this cep**Input** has made it clear that simply tweaking a few things is not enough. Instead, a holistic, overarching new approach is needed to reorganise European cloud policy and strengthen cybersecurity in Europe in the cloud age. In times of growing geopolitical uncertainty and security tensions, an erratic Trump administration that jeopardizes any planning security, as well as increasing conflicts over leadership in global technology, it is important to maintain and consolidate the EU's digital sovereignty and reduce dependencies without, however, depriving it of access to advanced digital services from third countries and thus falling behind in global competition.

[350] You can find more information on the new EU Commission here.

[351] Sarah Knafo advocates for a European cybersecurity criterion that takes sovereignty into consideration (in the case of sensitive data). She calls on the Commission "to align the 'high' level of the […] EUCS […] with the SecNumCloud certification requirements to ensure hosting providers are not subject to extra-European legislation" [European Parliament (2025)]. See also Kroet, C., EU cloud certification should mimic French scheme, says nationalist lawmaker, 27 February 2025, available here.

Centrum für Europäische Politik
FREIBURG | BERLIN

Authors:

Philipp Eckhardt, Head of the Financial Markets and Information Technology
eckhardt@cep.eu

Dr. Anja Hoffmann, LL.M. Eur., Policy Analyst, Internal Market and Competition
hoffmann@cep.eu

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Strasse 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN,
the **Centre de Politique Européenne** PARIS and
the **Centro Politiche Europee** ROMA form
the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

The Centres for European Policy Network analyses and assesses the policy of the European Union independently of individual or political interests, in alignment with the policy of integration and according to the principles of a free, market-based system.