Putting EU Digital Sovereignty and Single Market to the test:
A Voluntary EUCS High+ is crucial for
Competitiveness, Sovereignty and Digital Leadership

Cloud is the backbone of the digital economy and a key driver to boost European organizations' digital transformation and, consequently, their competitiveness. To achieve this and encompass new digital evolutions and use cases, in particular AI, European users must have the assurance that these evolutions are not happening without a suitable level of protection of data, including the most sensitive ones. This must be done at EU level to avoid Single Market fragmentation. With the new Commission in place and its clear commitment to digital sovereignty, discussions on the European Cloud Services Cybersecurity Certification Scheme (EUCS) should more than ever proceed with the inclusion of High+ criteria.

This would be fully consistent with the Draghi report, which has for instance recommended the adoption of a single EU wide policy for the procurement of cloud services by public administrations, including data residency requirements and requiring at a minimum EU sovereign control of key elements for security and encryption. This recommendation has also been reflected in the Mission Letter to the Executive Vice-President for Tech Sovereignty, Security and Democracy.

We, as cloud users and providers, representatives from various European countries, economic sectors and all sizes of companies, strongly support the inclusion of High+ criteria in the EUCS, for the following reasons:

- **Ensuring adequate data protection**. Such criteria would provide an EU-wide standard allowing users to have transparency, choice, and the necessary protection for their most sensitive data against access or operational disruption resulting from non-EU extraterritorial laws.

- **Guaranteeing freedom of choice**. A voluntary High+ EUCS would in no way exclude non-European providers, but simply offer an alternative to European cloud users. Users would retain the freedom to opt for such a level or not: this is about enabling user choice, not about restricting it. Public and private users would be able to opt for High+ for particularly sensitive data while selecting other levels for the rest. We fully support the voluntary and user-centric approach taken so far, which could be explicitly enshrined in the EUCS to avoid any residual doubt about the potential implications of harmonizing such criteria. Last but not least, an EUCS High+ standard would also be fully consistent with recently adopted Gaia-X standards.

- **Indispensable for cloud and AI uptake and successful EU digital transformation.** In the absence of such harmonised criteria, numerous users, including a very significant number of EU SMEs, would not be in a position to opt for cloud solutions. They would have to leave their data stored "on-premise" which would impede their digital transformation and capacity

to improve their cybersecurity capacities. Worse, they would be left with solutions that may be advertised as 'sovereign', but do not offer the protections they need. This scenario would significantly hinder cloud uptake and, hence, the development of common European data spaces and AI in the EU. This would, in turn, have a major impact on the EU industrial competitiveness. Moreover, it would disproportionately burden specific industrial sectors handling highly sensitive data as well as SMEs, which often lack the in-house capabilities and resources to come up with complex tailor-made solutions.

- **Avoiding Single Market's fragmentation.** The absence of an adequate High+ EU-level would further fragment the Digital Single Market into divergent national standards, inducing major administrative complexities and compliance costs and hitting all companies, especially the smaller ones. It would run against the Commission's overall simplification, competitiveness and Single Market priorities. It would also hinder European cloud providers to scale up their solutions in the Single Market. Any proposal aiming at keeping sovereignty requirements at national level (extension profiles, national labels) will therefore fail to address the issue.

The newly confirmed European Commission has committed itself to digital sovereignty. The EUCS puts the EU's commitments to the test. It is a first step, but a crucial one. It is an opportunity to achieve greater sovereignty in the cloud space and in AI – one that is user-driven and one that cannot be missed, if the EU wants to truly reduce its dependencies.

A significant number of EU Cloud providers and users across all sectors, nationality and sizes – including 45,000 European SMEs active in the digital sector – have voiced their strong support for the inclusion of such High+ criteria. Please refer for instance to the attached open letters and minutes from the Data Security event held on 26 September 2024, as well as to the eucshighplus.eu Internet site.

Therefore, we, as cloud users and providers and representatives from various European economic sectors, strongly support the inclusion of High+ criteria in the EUCS. At the very least, we call for a freeze of all EUCS-related discussions until an adequate alternative solution is found.


A1
AIRBUS
AIRFRANCE KLM GROUP
ALTER
aruba.it
ASD
AeroSpace and Defence Industries Association of Europe
BANQUE DE FRANCE
EUROSYSTÈME
Beltug
Caisse des Dépôts GROUPE
Capgemini
Cigref
RÉUSSIR LE NUMÉRIQUE
CIO PLATFORM NEDERLAND
clarence
CloudFerro
CRÉDIT AGRICOLE GROUP
CYBERNETICA
DASSAULT AVIATION
DASSAULT SYSTEMES
deep
DOCAPOSTE
Dutch Cloud Community
eDF
European DIGITAL SME Alliance
European Champions Alliance
EVIDEN
FINCANTIERI
FRANCE ASSUREURS
FAIRE AVANCER LA SOCIÉTÉ EN CONFIANCE
HarfangLab
informatique de la MSA et de ses Partenaires
IONOS
Klarrio
STREAMING AHEAD
LA POSTE GROUPE
LEONARDO
MBDA
Navantia


oesia grupo
odrive
OLMAR
GRUPOOLMAR
Open Nebula
orange
OVHcloud
Post Luxembourg
proximus
SAAB
SAFRAN
SAINT-GOBAIN
sck cen
secunet
SIPEARL
sopra steria
SPAC
STACKIT
tdf
telindus
a Proximus company
THALES
Building a future we can all trust
TIM
Tuxis
Internet Engineering
VEOLIA

Annex 1:
Previously Released Open letters

November 2023 Letter

EUCS: a crucial opportunity to provide European cloud users with full data protection and freedom of choice

Joint letter from European cloud users and providers

November 17th, 2023

We, European cloud users and providers, would like to reiterate our full support to maintain the inclusion of criteria that guarantee immunity against non-European extraterritorial laws in the voluntary European Cybersecurity Certification Scheme for Cloud Services (EUCS). This endorsement is rooted in our commitment to enhancing trust in the European cloud market and aims at giving users the freedom to choose the level of protection based on their needs and the level of sensitivity of their data.

The drive towards incorporating immunity to extraterritorial laws in cloud services is not industry-imposed but user-inspired and user-centric. **Recent data show that sovereign cloud solutions are a growing demand for European businesses:** around 70% of organizations perceived potential access to data by foreign authorities as a risk. This concern is particularly high in European countries such as Italy (75%), Sweden (72%), and Spain (71%).

The EU already hosts cloud providers with capacity to provide the highest level of cybersecurity and services needed by European organizations, regardless of whether their objectives are technical, commercial, or financial. More than one third of companies have already invested in sovereign cloud solutions, and nearly half plan to do so in the near future[3], which shows a willingness among organizations to address sovereignty issues.

This trend demonstrates an awareness and a proactive approach among EU public and private organizations towards solutions guaranteeing the level of data security and protection they need, depending on the level of sensitivity of their data. **By aligning the EUCS with these users' preferences, we ensure that the scheme remains relevant, responsive, and rooted in the actual needs of the European digital economy, where multicloud strategies are becoming the standard**.

Immunity requirements are already part of some existing national certifications: **the EUCS is not a departure from current practices and existing national cloud certifications, but an evolution towards a unified standard enhancing clarity and consistency across the**

European market. The introduction of immunity criteria within a voluntary scheme serves to complement rather than overshadow non-sovereign services.

This harmonization is not only beneficial for users but also for providers. **A European-level scheme prevents fragmentation across Member States, enhances competitiveness and transparency, and helps users understand cloud solutions based on their specific needs, including protection of their data's integrity with respect to third-country's jurisdiction**. It will also reduce certification costs, which is most beneficial for smaller entities with limited resources.

We aim to achieve a harmonized, EU-wide standard that provides clarity and choice, enhancing the scheme's usability and applicability, and that complies with the WTO's General Agreement on Trade in Services (GATS) which recognizes exceptions for privacy and individual records protection.

We understand that there are discussions around excluding from these requirements NATO member countries as well as countries with EU data adequacy agreements. The EUCS is not a cyberdefence instrument but a cybersecurity one, aimed at improving the functioning of the EU internal market. The EUCS goes much beyond NATO's remit and its criteria should not be conditioned to a military alliance. In addition, **mixing the EUCS and EU data adequacy agreements does not make sense since the EUCS does not cover personal data only, contrary to the GDPR and EU data adequacy agreements**, and in particular the recently agreed Transatlantic Privacy Framework.

The EUCS is a unique opportunity to strengthen the European cloud market by integrating harmonized user-driven needs for data protection against extraterritorial interference, with explicit and transparent criteria. **This scheme, grounded in existing market practices and user preferences, is set to play a pivotal role in shaping a secure, resilient, and competitive digital Europe.**

Sincerely,

(Alphabetic order): 3DS Outscale, Airbus, Aruba S.p.A., Atempo, Cloud Temple, Deutsche Telekom, Docaposte, EDF, Hexatrust, Ionos SE, Nameshield, Numspot, Oodrive, OpenNebula Systems, Orange, OVHcloud, Shadow, Tehtris, TIM.


AIRBUS
OUTSCALE
aruba.it
ATEMPO
CLOUD TEMPLE
DOCAPOSTE
EDF
HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY
IONOS
nameshield
Online Assets Security
NumSpot
Cloud. Européen. Citoyen.
odrive
Open Nebula
orange
OVHcloud
shadow
TEHTRIS
FACE THE UNPREDICTABLE
TIM

April 2024 Letter

EUCS: Ensuring full transparency and protection for European cloud users' most sensitive data is critical

A joint action from European Cloud Providers and Users

Deliberations on the candidate EU cybersecurity certification scheme on cloud services (EUCS) have been ongoing since December 2019. Much of the discussions have been centered around the inclusion of immunity / sovereignty requirements. **As European cloud providers and users committed to EU's digital competitiveness, we have been consistently advocating for the integration of transparent and harmonized requirements at the highest evaluation level of the EUCS scheme to protect the most sensitive European data against unlawful access.** Keeping in mind that EUCS is conceived as a voluntary certification scheme, we believe it should be grounded in existing market practices and user preferences while bringing transparency and protection to users where needed.

We believe the inclusion of sovereignty requirements is necessary to overcome market fragmentation, protect European organizations' most sensitive data, and encourage the development of sovereign cloud solutions in Europe. **Removing any reference to sovereignty provisions from the main scheme (including if shifted to an International Company Profile Attestation, ICPA) clearly fails to meet these objectives.** This would not only contradict what has been proposed in the previous EUCS schemes for over two years, but also give up the collective efforts undertaken by ENISA, the European Commission and Member States' representatives. The EU must not abandon its overall objective of fostering digital sovereignty, a goal that is all the more relevant in a context of geopolitical uncertainty.

We therefore urge Member States to reject any proposals that remove sovereignty requirements from the main body of the EUCS scheme for the following reasons:

1. **Addressing the risk of unlawful data access:** the inclusion of EU-HQ and European control requirements in the main scheme is necessary to mitigate the risk of unlawful data access on the basis of foreign laws, incompatible with the GDPR. The removal of these criteria from the main body of the scheme (including from a potential level high+/EL-4) means that adherence to EU sovereignty is no longer required for certification and that all cloud providers can potentially be certified at the highest security level of EUCS, even if they are subject to extraterritorial legislation (e.g. Chinese National Intelligence Law or US CLOUD Act). The result is that the risk of unlawful access remains unaddressed by the certification itself.

2. **Ensure consistency across the EU market:** harmonization of sovereignty requirements in Europe can only be achieved by setting out a uniform set of provisions in the main body of EUCS, enhancing clarity and consistency across the European market. Shifting this responsibility to national procurement officers (e.g. as suggested in the Belgian's Center for Cybersecurity concept note) who are supposed to decide for themselves which 'sovereignty elements' they deem necessary (or not) will inevitably lead to fragmentation. Contrary to the objective of EUCS, i.e. to bring more harmonization, the result will be different requirements at national level and,

consequently, legal, technical, and economic uncertainties for both EU cloud providers and users in the implementation of their cloud strategies.

3. **Offering users' clarity and transparency:** cloud users require transparency about the level of protection of their data. There is a high likelihood that users will rely on the certification scheme to ensure that their data is adequately secured. However, if a future EUCS scheme will leave the risk of unlawful data access unaddressed, this may lead to situations where cloud users will simply rely on the highest level without being adequately protected or informed about the risk of unlawful access stemming from extraterritorial legislation. This will ultimately impede investments in sovereign cloud solutions.

Including a clear and uniform set of sovereignty requirements in the main body of the EUCS is fundamental to support transparency, user choice, and the availability of alternative cloud solutions that are built in conformity with sovereignty requirements. On the contrary, **removing such requirements from the scheme would seriously undermine the viability of sovereign cloud solutions in Europe – many of which are either in development or already available on the market.** It would also impede European customers from being able to identify with certainty sufficiently secure solutions for their sensitive applications.

Moreover, **it would be inconsistent with European legislation such as the recently adopted Data Act[1] and important initiatives such as Gaia-X.** The GAIA-X policy rules, which were inter alia designed to ensure data sovereignty, explicitly include both an EU-HQ (criterion P5.1.4) and European control (criterion P5.1.5) requirement at the highest assurance level (label level 3). GAIA-X therefore sets a blueprint for EUCS, one that was jointly developed and adopted by cloud providers and users in Europe.

We therefore urge policymakers to take the necessary time to fully take into account the implications of a potential removal of sovereignty provisions from the main body of the EUCS scheme for European cloud providers and users as well as for the protection of Europe's most sensitive data as a whole. A digital and sovereign Europe requires access to the best cloud technologies while supporting the development of sovereign cloud solutions in Europe. We do believe these two goals can go hand in hand by supporting the inclusion of a harmonized set of sovereignty requirements in the framework of a voluntary EUCS scheme.

Sincerely,

A1, Airbus, Aruba S.p.A., Capgemini, Dassault Systemes, Deutsche Telekom, EDF, Exoscale, Ionos SE, OpenNebula Systems, Orange, OVHcloud, Proximus, Eutelsat Group, Sopra Steria, StackIT, TIM.

Annex 2:
"Data security in the cloud: a matter of competitiveness and resilience"
Event on September 26th, 2024

Organized by:

On September 26, 2024, the European Economic and Social Committee (EESC) hosted the event "Data Security in the Cloud: A Matter of Competitiveness and Resilience" - bringing together cloud users and providers, policymakers, and industry experts to address the growing need to protect sensitive data from extraterritorial legislation.

In this context, several European professional associations and companies were given the opportunity to present their perspectives from a cloud user perspective on the importance of incorporating voluntary High+ criteria into the European Cybersecurity Certification Scheme for Cloud Services (EUCS).

Danielle Jacobs, CEO of **Beltug** (association of CEOs and digital technology leaders in Belgium) emphasized that, through her daily interactions with members in various sectors such as banking, healthcare, and public services, cybersecurity has emerged as a top priority for IT users in Belgium. Danielle noted that while data is increasingly being migrated to the cloud, there remains a significant imbalance between cloud providers and users, particularly when it comes to negotiating vendor lock-ins. This situation is especially concerning given that a large majority of EU companies rely on non-European cloud providers. A recent survey by Beltug found that 94% of respondents expressed concerns about data security, with 78% worried about sensitive information being stored outside of the EU. Despite GDPR's focus on personal data, there is still a lack of effective solutions to protect business-sensitive information across the EU and the US, presenting a considerable challenge. In this context, Ms. Jacobs argued that companies should have the option to protect sensitive data through a voluntary, harmonized, cross-border approach and supported the need for High+ criteria to be included in the EUCS.

Sebastiano Toffaletti, CEO of the **European Digital SME Alliance** (association representing around 45 000 digital SMEs across the EU) recalled that they have discussed for months with their memberships and national trade associations and concluded that the EUCS is an important topic, not just for them, but for everyone. He notably stressed that " We do not have in

Europe the technological stock and the central element which is cloud computing ; our future sovereignty and economic prosperity and democracy is at stake because of that. The good news is that there are solutions to regain sovereignty and regain economic prosperity. [...] What we miss in Europe is a strong leadership, a strong industrial strategy. [...] In this context, the inclusion of High+ criteria into the EUCS is a very important piece of the puzzle. With the right sovereignty requirements in place, we could give a big boost to our cloud industry which could become a very important layer in the European technological stack we are missing."

Ulrich Ahle, CEO of **Gaia-X**, highlighted that facilitating data sharing among entire business communities necessitates both trust and standardized interoperability grounded in a European framework. This is particularly crucial as it sets the stage for Artificial Intelligence and notably Generative AI, on which Europe needs to be present and which depends on trusted data. 180 development projects for different data spaces in 16 different verticals (healthcare, Mobility, Manufacturing, etc.) are currently ongoing in Europe. Each of these data spaces has a governance authority based on commonly agreed rules. The recently adopted Gaia-X Compliance Document plays a central role in Gaia-X functioning, outlining various levels of conformity, including a highest level 3 that requires providers to comply with the equivalent of High + requirements to avoid extraterritoriality concerns. Level 3 is also a voluntary standard and was developed based on a clear demand from a proportion of Gaia X members (Cloud users). The Compliance Document is anticipated to shape future requests for proposals (RFPs) for cloud solutions. As market conditions evolve, it offers a potential framework for structuring the EUCS, illustrating how ambitious requirements can be achieved while promoting interoperability across different data spaces. Mr. Ahle anticipated that a limited proportion (which could be in the range of 5% of the user demand) would be placed under Level 3.

Emmanuel Sardet, representing **Crédit Agricole Group** (international banking group headquartered in France and the world's largest cooperative financial institution) and CIGREF explained that his company heavily relies on hyperscalers' landing zones worldwide. In this context, they require High+ criteria for both technical and legal reasons, as well as to avoid market fragmentation and cost uncertainties that could significantly affect bank profitability. "We will do our part by supporting the ecosystem adopting an EU regulation including High+ criteria. This cannot be overlooked: it has to be thought thoroughly and we will be happy to support that thinking" Mr. Sardet concluded.

Alfredo Nulli, representing **Telecomitalia** emphasized the need for clarity regarding sovereignty criteria among their customers. He pointed out that ambiguous criteria create uncertainties in the pricing of cloud services. In this context, Telecomitalia, drawing on its experience as a shareholder in the Italian cloud for the public sector over the past two years, advocates for the establishment of a clear framework at the EU level through the inclusion of High+ criteria in the EUCS.

Bart Moerman, representing the **Belgium Federation of Notaries**, stressed that sovereignty is one of the most pressing issues for his organization regarding the cloud. While in some countries, sovereignty is equated with locality and treated as a national concern rather than a

European one, he urged the EU to establish a unified regulation on sovereignty requirements in the cloud.

Claudia Gherman, representing **ASD** (European aerospace and defence professional association), strongly advocated for High+ criteria in EUCS: "For our industry, High+ criteria guarantees and protects the availability of most sensitive data against risks such as unregulated and unmonitored cloud storage and computing beyond EU's territory." She added that in ASD's view, since the EUCS is a voluntary scheme, the inclusion of High+ criteria will not distort the market, but the existence of this criteria would actually provide a unified EU reference to cloud users.

Valentin Mauboussin, representing **Veolia** (company headquartered in France with activities in water management, waste management and energy services operating in 18 EU countries), stressed that "Veolia strongly supports the inclusion of High+ criteria into the EUCS for three reason: ensuring a high level of protection for the sensitive data of our customers, reducing market fragmentation and preserving an agnostic cloud environment that is able to answer to our specific needs. We want to have a system in which we can freely determine which cloud providers better respond to our needs."

Kalman Tiboldi, representing **TVH** (company headquartered in Belgium supporting different industries in the aftermarket for service and maintenance, distributing spare parts in 182 countries), explained that machinery has begun to evolve into smart machines. These machines generate data, including high-value personal and non-personal information, and cross borders, which makes it very challenging for TVH to apply the appropriate data protection regulations. In this context, the implementation of a single regulation at the EU level, which includes the adoption of High+ criteria, would be a game changer.

Sabine Gielens, representing **VNO-NCW** (the largest employers' organization in the Netherlands), argued that the inclusion of sovereignty criteria in the EUCS should not be left to the discretion of a working group, but rather should be the subject of political discussion.

Pia Kraus, representing **Stakit, from the Schwarz Group**, reported that in recent years, the companies under Schwarz Group have evolved into an ecosystem that encompasses the entire value cycle, now also offering IT and cloud solutions not only for the ecosystem but also for third parties. This evolution is fueled by the strong belief that digital sovereignty in Germany and Europe is crucial. Ms. Klaus then called on the EU to "create an environment for companies to develop in the single market, leveling the playing field. This means establishing harmonized criteria to address market fragmentation, including sovereignty criteria in the EUCS."

Thierry Lelégard, representing **Si Pearl** (company manufacturing high-performance low-power microprocessors for supercomputing and artificial intelligence with locations in France, Germany, Italy, Spain and soon Romania), pointed out the importance for his company to preserve its sensitive data from non-European competition, including industries notoriously supported by extraterritorial laws in their countries. Because of the uncertainty created by the

absence of criteria like High+, Si Pearl had to build and operate its own data centers at a cost of 18 million euros, which is a major handicap for a scale-up company. "Not having High+ criteria is actually an obstacle to innovation in the EU" Mr. Leléguard insisted.

Daniel Sanchez, representing **A1 Group** (telecommunication company headquartered in Austria operating in Austria, Bulgaria, Slovenia and Croatia) stressed the strong demand for clarity and transparency among customers, which led his company to support the inclusion of High+ criteria in EUCS. He said: "With compliance and transparency, not only are you tackling to great extent topics such as pricing transparency with cloud providers, but you will also tackle investment needed in strengthening- the digital infrastructure for Europe in order to ensure that the data single market expands and is strengthened."

Jérôme Balmes, representing **France Assureurs** (French Insurance Federation, bringing together 252 insurance and reinsurance companies operating in France and covering over 99% of the market) highlighted that insurers handle a lot of data, and a small part of this data could benefit from High+ storage options. He thus expressed his organization's support to High+ criteria as long as the choice to use High+ providers remains voluntary.

Dries van Dyck, representing **SCKCEN** (Belgian nuclear research center), explained that his organization was increasingly being pushed towards the cloud while needing to store very sensitive data which falls in two categories. The first is data related to the security of the nuclear material it has on site. The federal agency of nuclear control (regulator) does not allow that kind of data to be stored in the cloud and people that (can) access it need to be vetted. The second is high value intellectual property (IP): the nuclear knowledge produced by SCKCEN is a prime target for economic espionage. Dr. Van Dyck said it would thus welcome having strong guarantees in regard to who manages its data as well as technical guarantees regarding the confidentiality of that data.

Pascal Rogiest, representing **Clarence** (created upon the initiative of Proximus with the support of the Luxembourg and Belgium governments), highlighted that sovereignty criteria are not only for protection purposes. It also meets a demand from cloud users, especially finance companies in Luxembourg, who see it as a way to differentiate themselves by bringing trust to their customers. They also expect cloud providers to be able to implement technologies like artificial intelligence in a secure environment. "That will not go through without High+ criteria" Mr. Rogiest concluded.

Another **Proximus** representative (provider of digital services and communication solutions operating in Belgium) further reminded that bringing High+ criteria in the EUCS is not a risk for customers, adding: "We do see the demand and we strongly believe that service providers must also make sure to provide an answer to it".

Dominique Grelet, representing **Eviden** (company headquartered in France providing services and products of cybersecurity across 69 countries), outlined the concerns of the customers regarding the ability to use a trustworthy cloud infrastructure. In response, Eviden is developing

products ensuring the encryption of data as well as managing the access and the users' identity and access, while also supporting the cloud users Joint Letter calling for the inclusion of High+ criteria in EUCS. This should remain "high on the list" according to Mr. Grelet.

Fabrice Le Saché, VP of **MEDEF** (the largest employer federation in France, representing 200 000 companies and 10 millions workers), stressed that digital transition cannot happen without safeguarding companies' sensitive data. With cloud computing becoming widespread in business, the issue of extra-European countries asserting jurisdiction over this data is critical. He emphasized the need for clear regulatory guidelines, which High+ is proposing to create a trustworthy cloud environment. The EU has been complacent, as indicated by the Draghi report, and urgently needs to take action to improve its digital sovereignty. Without a robust regulatory framework, European companies may face significant challenges in the next 5 to 10 years. This effort is not about nationalism, Mr. Le Saché said; it’s about developing reliable solutions for businesses.