November 2021

BSA | THE SOFTWARE ALLIANCE'S COMMENTS TO ANSSI ON SECNUMCLOUD (VERSION 3.2.A)

BSA | The Software Alliance[1] welcomes the opportunity to provide comments on the update draft SecNumCloud reference framework (version 3.2.a) given its important role in supporting robust and harmonized cybersecurity standards across industry, and implementing France's new Cloud Strategy. The fact that SecNumCloud is built among others on existing widely adopted, internationally recognized, risk management based and voluntary standards such as ISO/IEC 27001, allows for the evaluation of providers according to consensus criteria based on well-established industry best practices. Drawing from cloud-specific updates in ISO 27017 and 27018 would also help ensure interoperability and assurance of security compliance.

However, the draft version 3.2.a contains new requirements related to localization requirements and immunity to extraterritorial legislation that raise significant concerns:

- From an operational perspective, they could dramatically impact customers' ability to select the cloud service provider (CSP) that best meets their operational needs and provides state-of-the-art cybersecurity protections;
- From a commercial perspective, it might greatly increase the cost of compliance and oversight without adding to security outcomes: how the data is protected is more effective than where it is stored;
- From a legal perspective, some of the draft requirements raise serious questions of compatibility with existing EU legislation and international trade commitments.

We encourage ANSSI to consider all the above-mentioned aspects as it revises SecNumCloud. In particular, this national effort should fully align with ENISA's development of the cybersecurity scheme for cloud services (EUCS), as mandated under the EU Cybersecurity Act and avoid any further market fragmentation between Member States.

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that help businesses of all sizes in every part of the economy to modernize and grow. With headquarters in Washington, DC, and operations in more than 30 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. Follow BSA at @BSAnews.

BSA's members include: Adobe, Akamai, Atlassian, Autodesk, Bentley Systems, BlackBerry, Box, Cloudflare, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

5.3. Risk assessment

[…]

c) The service provider must take into account in the risk assessment:

- *the risks of breach of the confidentiality of commissioning entity data by third parties involved in the provision of the service (suppliers, subcontractors, etc.).*

d) The service provider must list, in a specific document, the residual risks associated with the existence of extraterritorial laws aimed at collecting data or metadata from commissioning partners without their prior consent.

e) The service provider must make available to the commissioning entity, at the latter's request, the elements for assessing the risks linked to the submission of the data of the commissioning entity to the law of a non-member state of the European Union.

BSA response:

Provision 5.3.d refers to "the existence of extraterritorial laws aimed at collecting data or metadata from commissioning partners without their prior consent." This scoping of extraterritorial laws relevant for the risk assessment is very broad and could encompass many laws that underpin legitimate government agencies action, including that of French government agencies.

First, regarding the criteria of data and metadata collection, the definition would include laws that underpin regulatory cooperation between France and EU Member States and/or Third Countries in areas such as competition, anti-money laundering and cooperation for criminal investigations.

Second, the criteria of extraterritorial application relates, in public international law, to a situation in which a State claims to apprehend, through its legal order, elements located outside its territory and vice versa let the authority of a foreign state exercise over its own territory. By definition and in the context of the risk assessment provisions of the SecNumCloud reference framework, this applies to laws from any given country that is relevant with regards the provider's service parameters. By default, that would include any extraterritorial laws from France, all the EU Member States and any other relevant third country.

Coupling the two criteria together therefore means that the risk assessment as currently drafted will require service providers to include national security laws, including the French intelligence law (reference: LOI n° 2015-912 du 24 juillet 2015 relative au renseignement[2]) which Art. L. 811-2 reads: "[Specialized intelligence services'] missions, in France and abroad, are to research, collect, use and make available to the Government information relating to geopolitical and strategic issues as well as threats and risks likely to affect the life of the Nation."

This approach helpfully avoids discriminating against any given EU member state or Third Country, an approach that would otherwise arguably be inconsistent with European and international law principles and public policy exemptions applicable to France. Going beyond this listing approach would create a significant additional burden on both the service provider who would be required to compile a comprehensive and accurate list, and on ANSSI who would need to have a complete and accurate picture of relevant extraterritorial legislations in scope as frame of reference.

However the chosen approach of a list to be provided by the service provider to its customer will generate a significant burden onto service providers regardless of their size or headquarters' location. It will also raise implementation challenges as cloud service providers do not have unfettered access to the data stored in their cloud infrastructure or service in a way that would enable them to

[2] See Art. L. 811-2.

determine which extraterritorial laws would be relevant in this context, at a time when the proposed Digital Services Act in its Article 7 seeks to prevent general monitoring obligation of information which providers of intermediary services transmit or store.

9.7. Restriction of access to information

d) In the context of technical support, if the actions necessary to diagnose and resolve a problem encountered by a commissioning entity require access to the data of the commissioning entity, then the service provider must:

- […]

- check that the person to whom access must be authorized is located within the European Union;

12.13. Remote diagnosis and remote maintenance of infrastructure components

a) In the context of remote diagnostics or remote maintenance of infrastructure components, considering the risks of breaching the confidentiality of commissioning partners' data, then the service provider must:

- […]

- check that the person to whom access must be authorized is located within the European Union;

BSA response to 9.7 and 12.13:

Diagnostics and mitigation measures rely on service providers' ability to use all their capabilities of threat detection, analysis and forensics, response and mitigation – regardless of where staff and capacities are located or time of day. Restricting the ability to conduct this type of actions to persons physically located in the European Union, or a particular country within the EU, would make this very difficult, if not impossible. 24/7/365 support requires resources in multiple time zones. This would dramatically hamper the ability of many CSPs, including those with headquarters in Europe and capabilities outside the EU, to draw from their global capabilities and to provide state-of-the art service. The same considerations would apply to second line support (patching code, testing, etc.), as data will need to flow between the customer in France and relevant service providers teams of engineers, which may be distributed across the globe.

In addition, international trade rules applicable to cloud service provisions require a commitment to principles of non-discrimination and national treatment in terms of the nationality of persons, products, services, or technologies. Subject to legitimate public policy limitations, a rule impacting the provision of cloud services would raise concerns if it distorted the market or altered conditions of competition based on the national origin of the persons, the products or services, or the technologies involved. In some cases, concerns may also arise if data transfer rules are designed to provide economic advantages to transfers within a country's borders, and to domestic persons, their products or services, or their technologies, than are afforded to cross-border transfers and non-national persons, products, services, or technologies.

For the foregoing reasons, we caution against some of the proposed requirements in the updated SecNumCloud draft reference framework for they impacts the provision of cloud services in a way that seems incompatible with the EU's and France's international trade commitments of non-discrimination against foreign persons, products, or technologies.[3]

[3] See most recently the EU-UK Trade and Cooperation Agreement, Chapter 2, Article DIGIT 6.

14.4. Secure development environment

a) The service provider must implement a secure development environment to manage the entire development cycle of the service information system.

b) The service provider must take into account the development environments in the risk assessment and ensure their protection in accordance with this standard.

14.5. Outsourced development

a) The service provider must document and implement a procedure to supervise and control the activity of outsourced development of software and systems. This procedure must ensure that the outsourced development activity complies with the provider's secure development policy and achieves a level of security for external development equivalent to that of internal development (see requirement 14.1 a).

BSA response to 14.4 and 14.5:

Standards and guidelines are important tools to help software developers assess and encourage security across the software lifecycle and to guide software security regardless of the development environment or the purpose of the software. It is important to address three distinct yet complementary functions: secure development to address security in the phase of software development when a software project is conceived, initiated, developed, and brought to market; secure capabilities to identify key security characteristics recommended for a software product; secure lifecycle to address considerations for maintaining security in a software product from its development through the end of its life. BSA strongly believes that both organizational processes and product security capabilities are vital elements of software security.

BSA developed and regularly updates the BSA Framework for Secure Software[4] (SSF) to offer an outcome-focused, standards-based risk management tool to help stakeholders in the software industry – developers, vendors, customers, policymakers, and others – communicate and evaluate security outcomes associated with specific software products and services. The SSF can be a useful reference tool to help service providers address requirements in 14.4 and 14.5.

19.2. Data localization

b) The service provider must store and process the data of the commissioning entity within the European Union.

c) The administration and supervision of the service must be carried out from the European Union.

d) The service provider must store and process technical data (identities of beneficiaries and administrators of the technical infrastructure, data handled by the Software Defined Network, technical infrastructure logs, directory, certificates, access configuration, etc.) within the European Union.

e) The provider may perform support operations from a state outside the European Union. It must document the list of operations that can be performed by the support from a country outside the European Union, and the mechanisms to ensure access control and supervision from the European Union.

BSA response to 19.2:

The requirement under point e) could contribute to increasing transparency, an approach that BSA supports. However, data localization or other highly restrictive requirements that affect the cross-border transfer of data do not advance cybersecurity (or data protection) goals and may trigger

[4] BSA Secure Software Framework, https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

unintended consequences. How data is protected is much more important to security than where it is stored. Cross-border data transfers are important for cybersecurity for several reasons. Companies may choose to store data at geographically diverse locations to obscure the location of data and reduce risk of physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location. In addition, cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. Mandating localization or restricting the ability to transfer and analyze data in real-time creates unintended vulnerabilities. Additionally, point (d) as currently drafted is not adapted to the provision of Software-as-a-Service offerings, and should further clarify which technical data would be required to be stored and processed in the European Union.

In addition, several EU legislations – including the Free Flow of Data Regulation and the General Data Protection Regulation – enshrine the free movement of data (personal and non-personal) within the EU and outward as a core principle of EU law. The EU Court of Justice has confirmed this principle, albeit with requiring additional safeguards in certain cases, in its Schrems II ruling.[5]
As already stated in our response to 9.7 and 12.13, localization requirements or other highly restrictive requirements would also run counter to EU (and therefore France's) international trade commitments. These commitments aim at ensuring that, unless limited protection of personal data and privacy policy exception applies, "*cross-border data flows shall not be restricted between the Parties by a Party:*

> *(a) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;*
> *(b) requiring the localisation of data in the Party's territory for storage or processing;*
> *(c) prohibiting the storage or processing in the territory of the other Party; or*
> *(d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory."*

19.6. Immunity to extra-community law

a) The registered office, central administration or main establishment of the service provider must be established in a Member State of the European Union.
b) The share capital and voting rights in the service provider's company must not be, directly or indirectly:
- individually held at more than 24%;
- and collectively owned more than 39%;
by third-party entities having their registered office, central administration or main establishment in a non-member state of the European Union.
These aforementioned third-party entities cannot individually:
- by virtue of a contract or statutory clauses, have a right of veto;
- by virtue of a contract or statutory clauses, designate the majority of the members of the administrative, management or supervisory bodies of the service provider.
c) In the event of recourse by the service provider, within the framework of the services provided to the commissioning entity, to the services of a third party company - including a subcontractor - having its registered office, central administration or main establishment within a State not a member of the European Union or belonging or being controlled by a third-party company domiciled outside the European Union, this aforementioned third-party company must neither have the

[5] Case C-311/18

practical competence to obtain the data processed through the service. These targeted data are those entrusted to the service provider by the sponsors as well as all technical data (identities of beneficiaries and administrators of the technical infrastructure, data handled by the Software Defined Network, technical infrastructure logs, directory, certificates, etc. access configuration, etc.) including information on the sponsors. For the purposes of this article, the concept of control is understood as being that mentioned in II of article L233-3 of the Commercial Code.
e) […]

BSA response to 19.6:

As a member of the WTO, France and the European Union have committed to abide by core principles of non-discrimination in the treatment of foreign persons, products, services, and technologies. Under Article III of the General Agreement on Tariffs and Trade (GATT), France and the EU have committed not to confer less favorable treatment on imported products vis-à-vis domestic products. Similarly, under Article 17 of the General Agreement on Trade in Services (GATS), France and the EU have committed not to confer less favorable treatment on non-national services and service providers vis-à-vis the treatment that they afford to national services and service providers. Among other sectors, these latter non-discrimination obligations apply specifically to all "computing and related services;" in other words, France did not stipulate any reservations or exceptions to its non-discrimination and market access commitments relating to foreign cloud services and cloud service providers, as well as all other computer-related services. Consequentially, several aspects of section 19.6 (including the local establishment, the capital and voting rights limitations, and the supervisory personnel stipulations) appear to contravene the commitments of France to afford foreign service providers full, unrestricted market access from a cross-border (Mode 1) and from a commercial presence (Mode 3) perspective in respect of all computing and related services.[6] In prior WTO litigation, WTO panels found that requirements very similar to those found in Section 19.6 breached WTO commitments and were required to be altered.[7]

Point 19.6.b) also appears to be a discriminatory criterion with no legal basis. It would violate EU rules such as the Public Procurement Directive 2014/24 and Article 14 of Directive 2006/123/EC on services in the internal market that expressly prohibits restriction based on the holding of the share capital.
It would also violate international public procurement rules such as the Multilateral Agreement on public procurement, making SecNumCloud highly challengeable before courts. In practice, publicly traded companies also have limited control and knowledge of the composition of their ownership precisely because of the share structure, which is also prone to continuously evolve over time. Point 19.6.b creates an additional burden on publicly listed companies - regardless of whether they are listed in France, in the broader EU and/or in third Countries - to monitor their shares' ownership. This requirement also appears in contradiction with capital market transparency laws which place transparency obligations onto shareholders.

For more information, please contact:
Isabelle Roccia
isabeller@bsa.org

[6] *See* European Union, GATS Schedule of Specific Commitments, GATS/SC/157, "Computer and Related Services," p. 58-62., at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/SCHD/GATS-SC/SC157.pdf&Open=True
[7] *See e.g.,* China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products, DS363, AB/R (Dec. 21, 2009), at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/WT/DS/363ABR.pdf&Open=True