ZWIĄZEK PRACODAWCÓW TECHNOLOGII CYFROWYCH LEWIATAN

Warszawa,26 maja 2023 r.
KL/206/89/AM/2022

Pan
Janusz Cieszyński
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Minister Cyfryzacji

Pan
Paweł Lewandowski
Podsekretarz Stanu
Ministerstwo Cyfryzacji

Szanowni Państwo,

W związku z pracami Grupy Roboczej ENISA nad opracowaniem schematu certyfikacji cyberbezpieczeństwa dla usług w chmurze oraz publikacją nieoficjalnej wersji projektu w tym zakresie, mając na uwadze zbliżające się spotkanie ECCG, Związek Pracodawców Technologii Cyfrowych przedstawia, w załączeniu, stanowisko wobec nieoficjalnej wersji projektu.

Z poważaniem

Jolanta Jaworska
Prezes Związku Pracodawców Technologii Cyfrowych Lewiatan

Do wiadomości:
Pan **Łukasz Wojewoda –** Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Pani **Katarzyna Prusak – Górniak –** Szefowa Referatu Cyfryzacji, Stałe Przedstawicielstwo RP przy UE w Brukseli

Załącznik: Stanowisko ZPTCL wobec nieoficjalnej wersji projektu schematu certyfikacji cyberbezpieczeństwa dla usług w chmurze

member of BUSINESSEUROPE

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

ZWIĄZEK PRACODAWCÓW TECHNOLOGII CYFROWYCH LEWIATAN

Summary of the main problematic proposals in the current version of the European Cybersecurity Certification Scheme for Cloud Services (EUCS)

A new version of the certification scheme for cloud services, EUCS, has been published. The text is still being analyzed and discussed, but we can already say that there has been no improvement or deletion of protectionist requirements. In particular, we consider the requirement for a European global HQ at the L4 level to be completely inadequate. Another big concern is that the L4 level will be used by default for a wider range of services than it "should be", e.g. even for financial services, which could lead to the disruption of business relations with providers from third countries.

The basic idea of cybersecurity certification at the EU level is to increase trust in products, services and processes in the field of information and communication technologies through their security. It is based directly on the Cybersecurity Act (Regulation 2019/881, CSA), which also includes 3 assurance levels – basic, substantial and high. In the EUCS proposal, the levels are defined as CS-EL1, CS-EL2, CS-EL3 and CS-EL4 (hereinafter referred to as L1, L2, L3 and L4), with L3 and L4 corresponding to the high level from the CSA.

We are convinced that the current definition of these 2 higher levels means a significant risk for maintaining the competitive environment on the European market. As for the highest L4, it is defined too deeply and broadly (p. 32):

„The CS-EL4 level provides reasonable assurance that a set of security controls is designed and operated in a way that goes beyond the CS-EL3 level to address security risks and threats related to data of particular sensitivity that would present risks to society if breached.

The data of particular sensitivity mentioned above cover:

- data related to secrets protected by law, for example, secrets relating to the deliberations of the Government and of the authorities reporting to the executive branch, to national defense, to foreign policy, to national security, to proceedings before the courts, or to the protection of privacy, to ***medical secrecy, and to trade secrets, which includes the secrecy of production methods, economic and financial information, and of information on commercial or industrial strategies****;*

- data that are necessary for the accomplishment of essential State functions, in particular the safeguarding of national security, the maintenance of public order and the protection of human life and health.“

Annex J is particularly problematic, on p. 306 it clearly requires that both the registered office of the cloud service provider (CSP) and the global headquarters must be established in the EU member state. This also applies to the processing and storage of data in the EU (p. 303, partially

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

also applies to L3). If this is not followed, the CSP cannot apply for L4 certification. This is a completely inadequate requirement given the L4 range definition above. In addition, we also perceive a certain conflict with the GDPR when it comes to the area of health and health information. The overlap with GDPR regulation should be explained and also why this certification proposal requires stricter rules than those required by GDPR (the proposal to use L4 for health information e.g. does not take into account Articles 45, 46, 47 GDPR). We also point out that already at the L3 level there is a requirement for all service personnel to be located in the EU and to pass certain reviews (see p. 304, requirement for L3: "passed an appropriate review"). This is a huge change and a burden for companies that will have to adapt without any delay.

Furthermore, the proposal at the highest L4 level aims to also include the commercial sector without limiting the size of entities. This issue has undergone extensive discussion in the Czech Republic during the preparation of cloud decrees, and the resulting consensus is that we are interested in a state cloud service provider, but only for a strictly defined set of systems in the country that are covered by the national highest security level 4. The private sector is in the area of cyber security requirements already regulated by the NIS2 directive, which defines in detail the gradation of requirements for large, medium, small and micro-enterprises. We see the general inclusion of "economic and financial information" in the scope of L4 certification requirements as unjustified, as it would mean in practice that, for example, information systems for corporate resource planning (ERP) in the private and public sector (without the application of a risk profile) should require L4 certification. It is also not clear to us how the L4 certification requirement for the protection of intellectual property and trade secrets will be applied in the public administration in a situation where all contracts must be published in the Register of Contracts. L4 should therefore focus only on critical infrastructure and clearly define only the most sensitive systems at the state level.

We also perceive as problematic the requirement that the CSP state in the contractual documents that it will only consider requests for investigations related to the provision of a cloud service that are issued on the basis of EU law or the law of an EU member state, already for the L3 level (p. 301). It is not possible to ask companies to disregard non-European requirements without adequate legal analysis. We believe that this contradicts the basic principles of a democratic state.

Furthermore, Annex H (p. 283) deals with the possibility of creating so-called Extension Profiles (CSEP). Unfortunately, this creates unlimited possibilities for the expansion of certification requirements and can thus cause significant fragmentation of requirements for CSPs across individual states. We also see a significant risk for the creation of a huge administrative burden

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

for companies. If this part were to remain in the proposal, it should ideally be limited only to L4 (in the current proposal, it can already be used for L2).

Final summary: SPČR has been supporting increasing the level of cyber security not only in the Czech Republic, but also in the EU. That is why we also support the basic idea of cyber security certification. Unfortunately, the current EUCS proposal does not correspond with this and, on the contrary, threatens to create unjustified protectionist barriers on the EU market, which will have a very negative impact on the competitiveness of the EU on the global market. We also see this as a risk for customers who could be exposed to rising service prices if there is not enough competition in the market offering the best services and products. Otherwise, the possibility of free choice would be limited, and with this comes the threat of reducing the innovation potential of the EU as a whole.

KL/206/89/AM/2022

member of BUSINESSEUROPE

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy