

20 iunie 2022

CĂTRE: **MINISTERUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII**
Domnului Sebastian-Ioan BURDUJA, Ministru

DIRECTORATUL NAȚIONAL PENTRU SECURITATE CIBERNETICĂ
Domnului Dan CÎMPEAN, Director

SPRE ȘTIINȚA: **MINISTERUL AFACERILOR EXTERNE**
Domnului Bogdan AURESCU, Ministru

REF: **Punct de vedere cu privire la Schema Europeană de Certificare a Securității Cibernetică pentru Servicii de Cloud (*European Cybersecurity Certification Scheme on Cloud Services – EUCS*)**

Stimați domni Miniștri,
Stimate domnule Director Cîmpean,

În numele Camerei de Comerț Americane în România (AmCham România), prin Comitetul pentru Economie Digitală, vă transmitem în cele ce urmează un **punct de vedere în contextul demersurilor la nivel european privind dezvoltarea schemei de certificare a securității cibernetică pentru serviciile de cloud** (*European Cybersecurity Certification Scheme on Cloud Services/EUCS*). Precizăm că, prin prezenta adresă, AmCham România se raliază [poziției formulate de Camera de Comerț Americană pe lângă Uniunea Europeană \(AmCham EU\)](#) împreună cu alte asociații de profil.

Comunitatea de afaceri pe care o reprezentăm susține eforturile autorităților naționale și europene de a răspunde provocărilor de securitate cibernetică și de a-și proteja cetățenii, instituțiile, organizațiile și mediul de afaceri în fața acestor provocări, prin instituirea unor mecanisme de certificare în domeniul securității cibernetică. În contextul în care Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) se apropie de finalizarea schemei pentru serviciile de cloud (EUCS), vă aducem în vedere o serie de îngrijorări cu privire la aspecte procedurale și de conținut. Aceste considerații vizează cu precădere potențialul includerii unor cerințe de „**suveranitate digitală**” și riscurile aferente atât pentru furnizorii internaționali și europeni de soluții de cloud computing, precum și pentru organizațiile care utilizează servicii de cloud și care necesită un nivel înalt de asigurare a securității cibernetică.

- Conform *Regulamentului privind securitatea cibernetică (Cybersecurity Act)*, **EUCS reprezintă un instrument tehnic și nu ar trebui compromis de considerații de natură politică**. În acest sens, considerăm că, indiferent de obiectivele de siguranță în baza cărora sunt fundamentate, includerea unor cerințe de „suveranitate digitală” în cadrul EUCS prezintă o conotație politică și un risc de creare a unor proceduri legale complexe pentru asigurarea conformării, în detrimentul obiectivului central al schemei, respectiv creșterea nivelului de securitate cibernetică;
- **Potențiala includere, în cadrul EUCS, a unor prevederi privind „suveranitatea digitală” respectiv localizarea și operarea serviciilor de cloud și a datelor exclusiv pe teritoriul Uniunii Europene, va limita eligibilitatea furnizorilor de soluții de cloud pentru cel mai ridicat nivel de certificare EUCS**. O astfel de limitare va genera obstacole pentru schimbul de date între diferite organizații, de altfel un instrument important pentru combaterea riscurilor de securitate cibernetică. Cerințele privind localizarea datelor vor crește costul menținerii celor mai noi soluții de stocare (*state-of-the-art solutions*) și vor reduce capacitatea alternativă de stocare a datelor în cazuri care implică scurgeri/pierderi de date sau întreruperi ale rețelelor;

- **Cerințele propuse prin EUCS, în special cele privind *data ownership* vor crea bariere substanțiale pentru intrarea pe piață a companiilor cu sedii în afara UE, precum și pentru companiile europene cu operațiuni internaționale și/sau globale.** Aceste bariere vor limita concurența pe piața serviciilor de cloud, vor crește costurile acestor servicii și vor reduce numărul potențialilor parteneri de tehnologie de încredere pentru mediul de afaceri din UE, în cele din urmă afectând capacitatea de inovare și de transformare digitală a UE;
- **Capacitatea actuală a pieței europene a serviciilor de cloud nu poate susține cererea UE pentru astfel de servicii, nici în ceea ce privește cantitatea, nici în ceea ce privește calitatea serviciilor.** Astfel, introducerea acestor reglementări va determina utilizatorii de servicii de cloud să se bazeze pe un număr limitat de furnizori care pot oferi soluții adecvate, riscându-se în acest mod crearea unor „concentrări economice inverse”. Asemenea concentrări economice vor avea un impact negativ semnificativ asupra abilității consumatorilor de a alege furnizori de tehnologie și de servicii de cloud care răspund cel mai bine nevoilor lor operaționale;
- **Statele Membre nu au ajuns la un consens în ceea ce privește introducerea unor cerințe privind „suveranitatea digitală” în schemele de certificare a securității cibernetice.** Câteva dintre Statele Membre își arată sprijinul pentru organizarea unor discuții care să definească și să clarifice o poziție politică comună privind suveranitatea digitală, în locul introducerii acestor cerințe în cadrul EUCS. Lipsa consensului între Statele Membre poate conduce la fragmentarea Pieței Comune, la reducerea încrederii și creșterea costurilor de conformare pentru industrie.
- **Procesul de dezvoltare a EUCS a fost marcat de un grad redus de transparență și de lipsa unei interacțiuni de substanță cu stakeholderii relevanți.** Rolul părților interesate, incluzând aici și reprezentanții industriei, precum și respectarea unor standarde internaționale dezvoltate consensual sunt vitale pentru asigurarea eficienței cerințelor privind securitatea cibernetică.

În acest sens, apreciem oportună o comunicare transparentă cu privire la stadiul discuțiilor privind dezvoltarea EUCS și recomandăm intensificarea dialogului între actorii relevanți din mediul public (autorități naționale de resort, Comisia Europeană, ENISA) și mediul privat, pentru finalizarea schemei și determinarea unei arhitecturi optime a EUCS, astfel cerințele introduse să servească în mod real obiectivului central, respectiv consolidarea securității cibernetice la nivelul Uniunii Europene.

În încheiere, reiterăm disponibilitatea de a fi un partener de dialog și vă asigurăm că puteți conta pe sprijinul și abordarea constructivă a AmCham România în definirea și fundamentarea poziției naționale cu privire la acest dosar european, precum și în demersurile ulterioare vizând operaționalizarea unor mecanisme de consolidare a securității cibernetice la nivel național. Pentru materializarea colaborării dintre instituțiile noastre, rămânem la dispoziția dumneavoastră prin Raluca Manea, Manager Politici Publice & Afaceri Europene (rmanea@amcham.ro / 0722.629.364).

Cu deosebită considerație,

Achilleas KANARIS

Președinte
Comitetul pentru Economie Digitală
AmCham România