EXPUNERE DE MOTIVE

Propunere legislativă privind consolidarea controlului asupra datelor din sistemele publice și protecția acestora în mediile de cloud și inteligență artificială

1. Necesitatea reglementării

Digitalizarea serviciilor publice impune măsuri verificabile pentru continuitatea activității, controlul subcontractării, gestionarea cheilor criptografice, evitarea blocării într-un singur furnizor și prevenirea accesului neautorizat la date. Proiectul inițial urmărea aceste obiective, dar propunea și localizarea prioritară pe teritoriul național, un certificat național obligatoriu, un nou cloud de stat și un mecanism de autorizare generală a solicitărilor din state terțe.
Aceste soluții necesită o justificare individualizată și pot genera conflicte cu dreptul UE.

2. Soluția legislativă

Propunerea reformulată înlocuiește obligațiile generale de localizare cu evaluări de risc pentru sistemele publice critice; introduce clauze contractuale minime, garanții privind accesul din state terțe, interoperabilitate și mecanisme de migrare; asigură informarea persoanelor vizate și accesul la servicii digitale pentru românii din străinătate; impune evaluări suplimentare la utilizarea inteligenței artificiale. Nu creează instituții sau scheme de certificare paralele.

3. Cadrul european și constituțional

Sunt relevante art. 26 și 148 din Constituție, art. 7 și 8 din Carta drepturilor fundamentale a UE, Regulamentul (UE) 2016/679, inclusiv art.1 alin.(3), art.32, 35 și 48, Regulamentul (UE) 2023/2854, Regulamentul (UE) 2019/881, Directiva (UE) 2022/2555, Regulamentul (UE) 2024/1689 și cadrul eIDAS astfel cum a fost modificat prin Regulamentul (UE) 2024/1183. Cerințele trebuie să respecte libera circulație a datelor, libertatea de stabilire, libera prestare a serviciilor, concurența și principiul proporționalității.
Normele privind securitatea națională, informațiile clasificate și prelucrarea în scop penal rămân distincte.

4. Practici europene relevante

Franța: doctrina „Cloud au centre" și calificarea SecNumCloud, administrată de ANSSI, ilustrează folosirea cerințelor de securitate și a evaluării expunerii la legislații extrateritoriale în anumite utilizări publice; nu reprezintă o obligație generală de localizare a tuturor datelor personale. Germania: catalogul BSI C5 oferă criterii de control pentru furnizorii cloud și probe de audit; nu echivalează cu o certificare unică obligatorie la nivelul UE. Italia: strategia națională cloud și clasificarea datelor și serviciilor administrației publice arată importanța diferențierii pe niveluri de criticitate. Estonia: infrastructura de interoperabilitate X-Road demonstrează utilitatea

schimbului securizat de date între registre, fără duplicarea centralizată a tuturor bazelor de date. Aceste exemple sunt orientative și trebuie reconfirmate în forma lor normativă actuală la data depunerii.

5. Impact social și administrativ

Măsurile urmăresc creșterea reziliență serviciilor publice, reducerea riscurilor de indisponibilitate și a costurilor de migrare, consolidarea protecției persoanelor și acces mai simplu la servicii pentru diaspora. Aplicarea se bazează în principal pe structuri și proceduri existente; nu se propune un nou registru centralizat al datelor personale.

6. Impact financiar și bugetar

Evaluarea sistemelor, auditul și adaptarea contractelor pot implica cheltuieli suplimentare. În lipsa inventarului infrastructurilor și a ofertelor de piață, nu poate fi prezentată o estimare numerică fundamentată. Înainte de depunere este necesară solicitarea datelor de cost de la autoritățile competente și elaborarea fișei financiare conform art.111 din Constituție și Legii nr.500/2002, după caz. Nu se prezintă drept certă neutralitatea bugetară.

7. Consultări și notificări

Se recomandă consultarea ANSPDCP, DNSC, ADR, ANCOM, a autorităților de achiziții publice, a Consiliului Legislativ și a Consiliului Economic și Social, potrivit competențelor. Necesitatea notificării în temeiul Directivei (UE) 2015/1535 trebuie analizată în funcție de caracterul eventualelor reguli tehnice sau reguli privind serviciile societății informaționale, anterior adoptării, dacă procedura este incidentă.

8. Concluzie

Propunerea consolidează controlul efectiv și securitatea datelor publice fără a institui o suveranitate teritorială absolută asupra datelor personale, noțiune incompatibilă cu structura dreptului UE și cu drepturile persoanelor vizate. Se solicită adoptarea propunerii legislative în forma anexată.

INIȚIATOR:

BAȘ ANA-MARCELA – deputat S.O.S.România

Tabel cu semnături la Propunerea legislativă privind consolidarea controlului asupra datelor din sistemele publice și protecția acestora în mediile de cloud și inteligență artificială

Nr.crt	Deputați/Senatori	Grupul parlamentar	Semnătura
	PASCA Ciprian Mihai	S.O.S. RO	
	BOȘ ANA MARIA	S.O.S. RO	
	CARAGAIA FLORIN	S.O.S. RO	
	OLTENASU SORIN	S.O.S. RO	
	TIU MIHAI-ADRIAN.	S.O.S. RO	
6	TOADER ELENA-LAURA	S.O.S. RO	
7	MACOVEI-ILIE SIMONA ELENA	S.O.S. RO	
8	IANEȚ Mariana	UPR	
9	Lazăroi Ioan	S.O.S. RO. -	
10	Racoș Enoch	Neo Filiat	
11	IONESCU TUDOR	S.O.S. RO	