Propunerea modificării proiectului de act normativ

Faptul că lipsește o analiză de impact asupra protecției datelor personale (obligatorie înainte de începerea prelucrării) face ca o serie de articole să propună aspecte care sunt contrare principiilor prelucrării datelor cu caracter personal din legislația actuală, conform GDPR.

Vă reamintim că printr-un HG nu se poate deroga de la normele imperative ale unui Regulament UE.

Din art 13 (4) b) rezultă că ADR este persoana imputernicita și UGC este operator, aceasta înseamnă ca se vor aplica conform toate obligațiile din GDPR - regulamentul 679/2016

Nr. Crt.	**Nr. articol**	**Textul propus de autoritatea inițiatoare**	**Conținut propunere / sugestie / opinie**	**Argumentarea propunerii / sugestiei / opiniei**
	Art 2 k)	**date sensibile** - sunt date a căror accesare, alterare, diseminare neautorizată sau indisponibilitate a accesului la acestea afectează îndeplinirea obiectivelor statului, pe termen mediu și lung		Deși este definit, termenul ”date sensibile” nu se regăsește în HG. Care este scopul? În temeiul datelor personale, **date sensibile** = date cu caracter personal din categorii speciale, deja definite în GDPR - regulamentul 679/2016 - **eventual schimbați termenul.**
	Art 3	asigurarea transparenței prin care proprietarii și administratorii datelor au controlul total asupra acestora și orice		Termenul de ”proprietarii datelor” nu este nici definit și nici nu e clar ce

Nr. Crt.	Nr. articol	Textul propus de autoritatea inițiatoare	Conținut propunere / sugestie / opinie	Argumentarea propunerii / sugestiei / opiniei
		operațiune de prelucrare a datelor este jurnalizată în vederea auditării ulterioare de către părțile autorizate;		este. Datele nu pot să aibă un proprietar, nici dpdv al dreptului comun (codul civil), nici dpdv al drepturilor de proprietate intelectuală. Nici termenul de”control total” nu este clar și nici nu poate fi implementat în cazul datelor cu caracter personal. Cu privire la jurnalizare, aceasta este o obligație legală pentru implementarea GDPR.
	Art 3.	prelucrarea sigură a datelor în cadrul serviciilor furnizate din Platformă cu garantarea specificării și limitarea scopului aferent fiecărei prelucrări de date, iar USC trebuie să adopte măsuri tehnice și organizaționale în scopul asigurării unui nivel adecvat de protecție a datelor	Termenul de ”specificare” nu există pentru scop, eventual refrazat - textul ar trebui limitat la date personale. “prelucrarea datelor personale respectand principiile obligatorii ale	Nu doar USC, ci și FSC au obligații de asigurare a securității datelor, inclusiv conform GDPR

Nr. Crt.	Nr. articol	Textul propus de autoritatea inițiatoare	Conținut propunere / sugestie / opinie	Argumentarea propunerii / sugestiei / opiniei
			Regulamentului UE 679/2016, inclusiv in ceea ce priveste limitarea legata de scop si asigurarea securitatii prelucrarii datelor personale”	
	Art 6	fără consimțământul USC,	fără **acordul** USC	USC este persoană juridica, nu persoană fizică. Consimțământul aparține exclusiv unei persoane fizice.
	Articol 7	(2) Responsabilitatea legală privind păstrarea datelor sau distrugerea acestora este a USC.		Răspunderea legală pentru datele personale este definită de GDPR, conform rolului avut - operator/imputernicit și nu poate fi schimbat printr-un HG. Termenul de **distrugere** se folosește exclusiv pentru datele personale pe hartie, pentru cele în format electronic vorbim de

Nr. Crt.	Nr. articol	Textul propus de autoritatea inițiatoare	Conținut propunere / sugestie / opinie	Argumentarea propunerii / sugestiei / opiniei
				ștergere.
	Articol 9	b) acces facil la rețea - funcționalitățile serviciilor de cloud sunt accesibile prin intermediul unei rețele de comunicații standardizate		Ce înseamnă "standardizat"? Vă referiți la rețele publice de comunicații electronice, care sunt reglementate de ANCOM (si implicit standardizate)?
	Art 12	La nivelul Platformei Cloud Guvernamental se stabilesc următoarele roluri:	Specificat rolul cetateanului in Platforma de Cloud Guvernamental.	Din text ar rezulta că cetățeanul - utilizatorul serviciilor USC - nu are niciun rol. Până la urmă platforma trebuie să fie în interesul cetățeanului, nu a USC sau FSC.
	Art 13	asigură listarea, administrarea și delistarea în marketplace a aplicațiilor și serviciilor disponibile în Platformă;		Dacă ADR este administratorul unui marketplace (termenul folosit în romana este de piață) unde persoane juridice pot adăuga aplicații, s-ar putea sa fie aplicabil Regulamentul

Nr. Crt.	Nr. articol	Textul propus de autoritatea inițiatoare	Conținut propunere / sugestie / opinie	Argumentarea propunerii / sugestiei / opiniei
				P2B al UE https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32019R1150&from=EN
	Articol 13	(3) FSC are următoarele responsabilități: f) informează USC cu privire la: i) rezultatele auditurilor de securitate, sub garantarea confidențialității; ii) incidente de securitate fizică și cibernetică și oferă suport adecvat, în limita competențelor, pentru gestionarea posibilelor riscuri de protecție a datelor prezentate de astfel de incidente, în termenii definiți în Acord în conformitate cu legea aplicabilă		Conform GDPR e invers - dacă FSC este împuternicit, USC are dreptul de audit - art 28 (2) h) in GDPR Iar un act normativ de rang inferior nu poate deroga de la aceasta obligație.
		) elaborează norme pentru gestionarea datelor procesate în Platforma de Cloud Guvernamental, în funcție de politicile de clasificarea datelor, inclusiv criterii tehnice și de securitat	Norma este contrara GDPR	Clasificarea datelor personale se face de Operator, nu de ADR, deci normele acestea nu pot să contravină instrucțiunilor operatorului.
	Articol 13	(4) Din perspectiva managementului datelor, ADR: FSC asigură monitorizarea evenimentelor de prelucrare a datelor cu caracter personal prin intermediul componentei		Nu era vorba că cetățenii află automat, direct din sistemul de jurnalizare, cine, când și

Nr. Crt.	Nr. articol	Textul propus de autoritatea inițiatoare	Conținut propunere / sugestie / opinie	Argumentarea propunerii / sugestiei / opiniei
		de jurnalizare și notifică USC cu privire la încălcarea protecției datelor cu caracter personal, fără întârzieri nejustificate, pentru ca USC să poată notifica, dacă este necesar, persoanele vizate afectate.		cum le-au prelucrat datele personale?
		) FSC asigură monitorizarea evenimentelor de prelucrare a datelor cu caracter personal prin intermediul componentei de jurnalizare și notifică USC cu privire la încălcarea protecției datelor cu caracter personal, fără întârzieri nejustificate, pentru ca USC să poată notifica, dacă este necesar, persoanele vizate afectate. i) FSC notifică Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal în termen de 72 de ore după ce FSC ia cunoștință de încălcare. FSC furnizează USC cel puțin următoarele informații:	Norma este contrara GDPR	USC are obligația să notifice în 72 de ore Autoritatea, și doar în anumite cazuri utilizatorii. i) este ilegal - obligația de notificare este doar a Operatorului, persoana împuternicită nu poate să notifice direct Autoritatea - vezi și ghidul EDPB în acest sens.
	Articol 14	USC are obligația să notifice în 72 de ore Autoritatea, și doar în anumite cazuri utilizatorii. i) este ilegal - obligația de notificare este doar a Operatorului, persoana împuternicită nu poate să notifice direct Autoritatea - vezi și ghidul EDPB în acest sens. de securitate cibernetică al infrastructurii de bază utilizată pentru	Notificare este obligație legală, dar remedierea ar trebui sa fie împărțită - probabil marea majoritatea a cazurilor va și FSC și STS.	De ce remedierea vulnerabilităților descoperite în IaaS și PaaS trebuie remediate de utilizatorii serviciilor de cloud? **Nu ar trebui să fie treaba FSC? Sau STS +**

Nr. Crt.	Nr. articol	Textul propus de autoritatea inițiatoare	Conținut propunere / sugestie / opinie	Argumentarea propunerii / sugestiei / opiniei
		furnizarea serviciilor de cloud pe model IaaS și PaaS din cadrul CPG, STS are următoarele Responsabilități: d) notifică USC, cu informarea ADR, cu privire la vulnerabilitățile de securitate, la adresa disponibilității, integrității și confidențialității, identificate la nivelul serviciilor de cloud IaaS și PaaS, în vederea remedierii acestora **de către USC**;		**FSC?**
	Art 17 (6)			Vă recomandăm sa nu includeți elementele contractuale (care sunt prin esența înțelegerea părților) intr-o lege! Dar pct j va trebui să fie mai mult, cu condițiile minime din art 18 GDPR.
	Art 26	API gateway		Poate ar fi bine să se clarifice cine verifică transferul datelor personale prin API Gateway - are ADR un rol?
	Art 31			Propunerea de

Nr. Crt.	Nr. articol	Textul propus de autoritatea inițiatoare	Conținut propunere / sugestie / opinie	Argumentarea propunerii / sugestiei / opiniei
				text pare a veni din zona de securitate, dpdv al datelor personale toate s-ar încadra la nivelul 3, dar atunci ar trebui o alta categorie pentru date cu caracter special
	Art 40	FSC, în calitate de persoană împuternicită, nu poate împuternici la rândul său un alt FSC sau o entitate parteneră decât cu acordul prealabil scris al USC		**Corect. Deci USC poate sa spuna ca nu vrea ca SRI sau STS să aibă acces la date, corect?**
	Art 41			Dincolo de datele prelucrate direct de USC, și FSC o să prelucreze date personale în special ca date tehnice ca urmare a prestării serviciilor - ele nu sunt acoperite nicaieri în acest HG.
	42	În scopul verificării legalității prelucrării datelor cu caracter personal, monitorizării și asigurării integrității și securității corespunzătoare a datelor cu caracter personal, USC are obligația de a stoca informații		Textul poate fi interpretat ca un **data retention**, ceea ce ar fi ilegal - obligația rezulta ca urmare a

Nr. Crt.	Nr. articol	Textul propus de autoritatea inițiatoare	Conținut propunere / sugestie / opinie	Argumentarea propunerii / sugestiei / opiniei
		cu privire la acțiunile de prelucrare derulate prin intermediul serviciilor de cloud furnizate în cadrul CPG. (2) Informațiile prevăzute la alin. (1) sunt stocate sub forma unor jurnale, loguri de sistem, și sunt prezentate în mod transparent și nemijlocit persoanei vizate, la cererea acesteia sau prin intermediul aplicației de notificare a prelucrărilor de date cu caracter personal, după caz		implementării GDPR, dar nu neaparat printr-o lege.
		Jurnalele de acces la date sunt păstrate pentru o perioadă de 36 luni de la data înregistrării acțiunii privind datele respective	Norma contrara GDPR	Termenul este stabilit de operator, nu de împuternicit!

Menţionăm că toate sugestiile transmise pentru textul de act normativ vor fi făcute publice, fiind parte dintr-un proces dedicat transparenţei decizionale. Doriţi ca numele dvs. să fie asociat cu aceste propuneri sau doriţi ca propunerile înaintate să fie anonime? Datele de contact nu sunt făcute publice.

|X| Doresc să fie menţionat numele organizaţiei/numele persoanei fizice (după caz).

|_| Doresc să fie anonime.