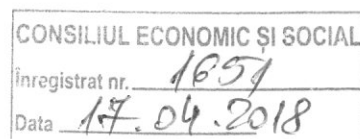
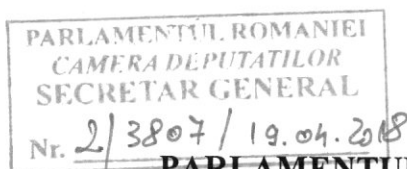


Membru fondator al Asociației Internaționale a Consiliilor Economice și Sociale și Instituțiilor Similare (AICESIS)
Membru al Uniunii Consiliilor Economice și Sociale și Instituțiilor Similare ale Statelor și Guvernelor Membre ale Francofoniei (UCESIF)

„Consiliul Economic și Social este organ consultativ al Parlamentului și al Guvernului în domeniile de specialitate stabilite prin legea sa organică de înființare, organizare și funcționare.” (Art. 141 din Constituția României revizuită)

Către,

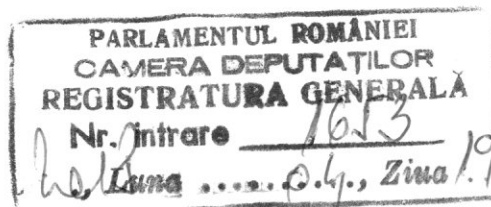


PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR

Doamnei Secretar General Silvia – Claudia MIHALCEA

Stimată doamnă Secretar General,



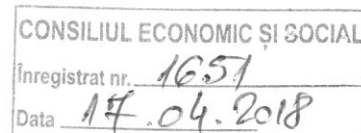
Referitor la adresa dumneavoastră nr. Plx167,Plx169/03.04.2018, înregistrată la Consiliul Economic și Social cu nr. 1504/04.04.2018, vă transmitem atașat avizul Consiliului Economic și Social referitor la *propunerea legislativă privind măsuri de punere în aplicare a regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/EC (Regulamentul general privind protecția datelor) (Plx167/03.04.2018).*

Cu deosebită considerație,

Silvia-Mihaela ARICIU

Director

Direcția Elaborare Avize și Pregătire Ședințe



AVIZ

**referitor la propunerea legislativă privind măsuri de punere în aplicare a
regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului
din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește
prelucrarea datelor cu caracter personal și libera circulație a acestor date
și de abrogare a Directivei 95/46/EC (Regulamentul general privind
protecția datelor) (Plx167/03.04.2018)**

CONSILIUL ECONOMIC ȘI SOCIAL

În temeiul art. 5 lit. a) din Legea nr. 248/2013 privind organizarea și funcționarea Consiliului Economic și Social, republicată, cu modificările și completările ulterioare, în ședința din 17.04.2018, avizează **FAVORABIL** prezentul proiect de act normativ, cu **propunerile de modificare și observațiile** prevăzute în anexă.

Președinte,

Iacob BACIU



Membru fondator al Asociației Internaționale a Consiliilor Economice și Sociale și Instituțiilor Similare (AICESIS)
Membru al Uniunii Consiliilor Economice și Sociale și Instituțiilor Similare ale Statelor și Guvernelor Membre ale Francofoniei (UCESIF)

„Consiliul Economic și Social este organ consultativ al Parlamentului și al Guvernului în domeniile de specialitate stabilite prin legea sa organică de înființare, organizare și funcționare.” (Art. 141 din Constituția României revizuită)

ANEXĂ

Propunerile de modificare și observațiile aferente

propunerii legislative privind măsuri de punere în aplicare a regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date și de abrogare a Directivei 95/46/EC (Regulamentul general privind protecția datelor) (Plx167/03.04.2018)

Nr. crt.	Text inițial	Text propus	Motivare
1.	Art. 3 – Prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea (1) Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri este interzisă, cu excepția	Art. 3 – Prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea (1) Prelucrarea datelor genetice, biometrice sau a datelor privind sănătatea, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri este interzisă, cu excepția prelucrărilor	Aceasta propunere de lege are o abordare restrictivă prin raportare la activitățile de profilare și decizie automată, bazate pe procesarea de date speciale (reglementate prin GDPR), aceste activități fiind interzise în mod expres în cazul operatorilor privați chiar și în ipoteza existenței consimțământului persoanei

prelucrărilor efectuate de către sau sub controlul autorităților publice, în limitele puterilor ce le sunt conferite prin lege și în condițiile stabilite de legile speciale care reglementează aceste materii, care să prevadă și garanții adecvate pentru persoana vizată. Interdicția nu poate fi ridicată prin consimțământul persoanei vizate.	efectuate de către sau sub controlul autorităților publice, în limitele puterilor ce le sunt conferite prin lege și în condițiile stabilite de legile speciale care reglementează aceste materii sau a prelucrărilor care au făcut obiectul unei analize de impact, care să prevadă și garanții adecvate pentru persoana vizată. Interdicția nu poate fi ridicată prin consimțământul persoanei vizate.	vizate. Înțelegem ca Statele Membre detin prerogativa reglementării suplimentare, mai stricte, în acest domeniu însă dorim să evidențiem faptul că aprobarea și, ulterior, aplicarea acestei prevederi poate avea un caracter blocant în unele zone de activitate (ed exemplu: domeniul asigurărilor, în care declarațiile persoanei vizate cu privire la starea de sănătate sunt relevante în procesul de stabilire a eligibilității și condițiilor pentru o poliță de asigurare de viață, caz în care fransiza sau alte componente ale pretului asigurării se calculează pe baza unui calcul actuarial care are în vedere și datele privind sănătatea). Având utilizarea noilor tehnologii în toate sectoarele de activitate și automatizarea, precum și utilizarea unor practici care să răspundă în mod simplu și rapid oricărei cereri adresate de persoanele fizice, apreciem că nu ar trebui introduse prevederi restrictive suplimentare celor prevăzute prin GDPR. În temeiul prevederilor considerentelor GDPR (71 teza finală): "Procesul decizional automatizat și crearea de profiluri pe baza unor categorii speciale de date cu caracter personal ar trebui permise numai în condiții specifice" și al Orientărilor WP 248 / 2017 referitoare la PIA (Privacy Impact Assessment), recomandăm ca prelucrarea acestor categorii sensibile de date să poată fi realizată în condițiile realizării în prealabil a unei analize de impact (PIA). De asemenea, propunem eliminarea imposibilității de a ridica interdicția prin
--	--	--

2.	Art. 4 – Prelucrarea unui număr de identificare național « (2) Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvaluirea documentelor ce îl conțin, în scopul prevăzut la art. 6 lit. f) din Regulamentul general privind protecția datelor, respectiv al realizării intereselor legitime urmărite de operator, sau de o parte terță, se efectuează cu instituirea, de către operator, a următoarelor garanții : (...) a) punerea în aplicare de măsuri tehnice și organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minim a datelor, precum și pentru asigurarea securității și confidențialității prelucrărilor de date cu caracter personal, conform dispozițiilor art. 32 din Regulamentul general privind protecția datelor; (...) c) aderarea la un cod de conduită aprobat, în condițiile art. 40 din Regulamentul general privind protecția datelor și asumarea respectării dispozițiilor acestuia ; d) stabilirea de termene de stocare în funcție de natura datelor și scopul prelucrării, precum și de termene specifice în care datele cu caracter personal trebuie sterse sau revizuite în	Art. 4 – Prelucrarea unui număr de identificare național (2) Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvaluirea documentelor ce îl conțin, în scopul prevăzut de art. 6 alin. (1) lit. f) din Regulamentul general privind protecția datelor, respectiv al realizării intereselor legitime urmărite de operator, sau de o parte terță, se efectuează cu instituirea, de către operator, a următoarelor garanții: (...) a) punerea în aplicare de măsuri tehnice și organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minim a datelor, precum și pentru asigurarea securității și confidențialității prelucrărilor de date cu caracter personal, conform dispozițiilor art. 32 alin 1-2 din Regulamentul general privind protecția datelor; (...) c) aderarea la un cod de conduită aprobat, în condițiile art. 40 din Regulamentul general privind protecția datelor și asumarea respectării dispozițiilor acestuia sau realizarea unui test de necesitate și implementarea măsurilor stabilite în urma testului pentru asigurarea prelucrării legale și echitabile; d) stabilirea de termene de stocare în funcție de natura datelor și scopul prelucrării, precum și de termene specifice	consimțământul persoanei vizate. Propunem completarea art. 4 alin.(2) din următoarele considerente: Referința exclusivă la principiu <i>minimizării</i> apreciem că nu este relevantă în contextul formulării și demersului dat (asigurarea măsurilor tehnice și organizatorice). Această afirmație își regăsește susținerea și prin raportare la existența sediului conceptual al materiei din Regulament – preambul pct.(78), (156), respectiv art. 5 alin.1 lit. c), art. 25 alin. 1, art. 47, alin. 2 lit. d). Suplimentar, celelalte principii asociate Regulamentului nu sunt tratate aici în niciun fel (ex. limitarea scopului, transparența, răspunderea, integritatea etc.). Apreciem că formularea propusă aduce aplicabilitatea dedicată principiilor dorit a fi protejate. c) Operatorii au opțiunea, dar nu și obligația, să adere la coduri de conduită, mai ales că nu toți operatorii sunt reprezentați de asociații și alte organisme. Mai mult, este probabil că va dura o perioadă până când vor fi finalizate și aprobate coduri de conduită după aplicarea Regulamentului general privind protecția datelor începând de la 25 mai 2018.
----	---	---	--

vederea stergerii ; e) instruirea periodica cu privire la obligațiile ce le revin, a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.	in care datele cu caracter personal trebuie sterse sau revizuite in vederea stergerii e) instruirea periodica cu privire la obligațiile ce le revin, a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.	În acest context, considerăm că ar trebui recunoscută posibilitatea operatorilor de a asigura definirea și asumarea măsurilor pentru respectarea Regulamentului și prin alte modalități decât prin aderarea la un cod de conduită aprobat. Testul de necesitate este o analiză ce trebuie realizată când un operator se întemeiază pe interesul său legitim în operațiuni de prelucrare, acest test fiind menit să asigure identificarea măsurilor necesare pentru a asigura echilibrul între interesele operatorului și potențialul impact asupra intereselor, drepturilor și libertăților fundamentale ale persoanelor vizate. Totodata, avand in vedere prevederile: Art. 32 (3) Securitatea prelucrării GDPR, conform carora “Aderarea la un cod de conduită aprobat, menționat la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.”, ex. referitoare la implementarea de măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului adus drepturilor si libertatilor persoanelor fizice, Consideram ca cerintele de la lit. a), lit. d) chiar si de la lit. de ar fi implicit indeplinite in cazul aderarii la un cod de conduita. d) Avand in vedere ca natura datelor este aceea
--	--	--

			de identificare, nu este clara referinta la «natura datelor » din cadrul propunerii de la lit. d) si propunem eliminarea acestei referinte. e) Operatorul/ persoana imputernicita trebuie sa stabileasca modul de instruire a persoanelor care prelucreaza date persoane sub directa lor autoritate. Reglementarea unei obligatii de instruire periodica, fara a defini periodicitatea si/sau fara a defini criteriile in baza carora aceasta poate fi determinata, are un caracter interpretabil și neclar.
3.	Art. 5 – Prelucrarea datelor cu caracter personal în contextul relațiilor de munca „În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaților, în scopul realizării intereselor legitime, este permisă numai dacă: a) interesele legitime urmărite de angajator vizează activități de importanță deosebită, temeinic justificate și prevalează asupra intereselor sau drepturilor și libertăților persoanelor vizate; b) angajatorul a realizat informarea prealabilă obligatorie, completă și în mod explicit a angajaților; c) angajatorul a consultat sindicatul sau, după caz, reprezentanții angajaților înainte de introducerea sistemelor de	Art. 5 – Prelucrarea datelor cu caracter personal în contextul relațiilor de munca „În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaților, în scopul realizării intereselor legitime, este permisă numai dacă: a) interesele legitime urmărite de angajator vizează activități de importanță deosebită, temeinic sunt justificate și prevalează asupra intereselor sau drepturilor și libertăților persoanelor vizate; b) angajatorul a realizat informarea prealabilă obligatorie, completă și în mod explicit a angajaților; c) angajatorul a consultat informat sindicatul sau, după caz, reprezentanții angajaților înainte de introducerea sistemelor de monitorizare; d) alte forme și modalități mai puțin	Modificările au în vedere următoarele: Angajatorul are drepturile prevăzute în art. 40 alin 1) litera a și b din Codul Muncii : « Angajatorul are, în principal, următoarele drepturi: a) sa stabileasca organizarea și functionarea unitatii; d) sa exercite controlul asupra modului de indeplinire a sarcinilor de serviciu; » In considerarea drepturilor sus-mentionate, care confera angajatorului dreptul de a institui o disciplina a muncii, angajatorul ar trebui sa poata monitoriza modul în care angajatii isi indeplinesc obligatiile de munca, sub conditia realizarii informarii prealabile obligatorii a angajatilor (lit.b). Criteriile din cadrul art. 5 contureaza ideea necesitatii unei evaluari a impactului asupra protectiei datelor, fara insa a mentiona expres acest lucru. Pornind de la prevederile art. 35 alin. (4) si alin. (5) din GDPR, consideram necesar ca

	monitorizare; d) alte forme și modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator nu și-au dovedit eficiența și e) durata de stocare a datelor cu caracter personal este proporțională cu scopul prelucrării, dar nu mai mare de 30 de zile , cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate.	intruzive pentru atingerea scopului urmărit de angajator nu și-au dovedit eficiența și monitorizarea este limitată în scop și proporțională scopului; e) durata de stocare a datelor cu caracter personal este proporțională cu scopul prelucrării, dar nu mai mare de 30 de zile ,cu aplicarea termenelor prevăzute de lege, după caz;. f) este desfasurata în vederea indeplinirii de catre angajator a unei obligatii legale.	ANSPDCP să realizeze și să publice lista tipurilor de operațiuni care : 1. -fac obiectul PIA 2. pentru care nu este necesară PIA 3. cazurile în care consultarea prealabilă a ANSPDCP este obligatorie (art. 36 alin. (1).GDPR) Ca referință avem Ghidul G29 WP 248 «Guidelines on Data Protection Impact assessment (DPIA) and determining whether processing is « likely to result in a high risk » for the purpose of Regulation 2016/679 (pg. 5 /ultimul paragraph și pagina 10/ ultimul paragraph). a) Sintagmele “activități de importanță deosebită” și « temeinic » sunt interpretabile, solicităm eliminarea acestora. Propunem completarea art. 5 alin.(1) pentru a clarifica domeniul de aplicare al acestui articol. Acest articol este menit să asigure o protecție sporită angajaților în cazul în care angajatorii ar dori să realizeze monitorizarea lor la locul de muncă. De reținut că pot exista sisteme de monitorizare prin mijloace de supraveghere electronice ce sunt menite și/sau folosite pentru protecția echipamentelor, iar nu pentru a stabili aspecte ce țin de comportamentul, performanța, localizarea sau deplasarea angajaților. De ex., există multiple soluții tehnice ce rulează automat și sunt menite să protejeze sistemele societăților împotriva atacurilor cibernetice și altor riscuri ce pot afecta securitatea datelor.
--	---	--	---

		c) În considerarea celor expuse anterior, apreciem ca nu este necesara consultarea sindicatului/—reprezentantilor salariatilor atata timp cat salariatii sunt informati în prealabil; de asemenea, o informare a sindicatului cu privire la utilizarea unor astfel de sisteme de monitorizare apreciem ca poate fi utila. d) Sintagma “alte forme si modalitati mai putin intruzive pentru atingerea scopului urmarit de angajator nu si-au dovedit eficienta » este interpretabila, nu avem reglementare de referinta si solicitam eliminarea acesteia. e) Durata de stocare a datelor cu caracter personal este proportionala cu scopul prelucrării si se analizeaza functie de fiecare caz. Impunerea unui termen general nu se justifica, cu atat mai mult in contextul in care pot exista situatii expres reglementate prin lege. Consideram ca durata de stocare este un element care va fi analizat in cadrul PIA (daca se va mentiona expres ca aceasta este necesara), care este cel mai probabil diferita de la o prelucrare la alta. Având în vedere că vorbim de o monitorizare circumscrisă unui scop, reprezentat prin interesul legitim al operatorului, apreciem că perioada de stocare de 30 de zile este foarte mică. De asemenea, apreciem ca termenul propus de 30 de zile poate fi greu de asigurat în cazul operatorilor ce au operațiuni în sedii multiple.
--	--	---

f) Pentru situația îndeplinirii unei obligații legale nu există prevederi exprese în dreptul intern și consideram ca este necesară o astfel de prevedere.

dacă impunerea unor condiții mai drastice în ceea ce privește prelucrarea datelor cu caracter personal în cadrul relațiilor de muncă se justifică în ipoteza supravegherii prin mijloace video, nu același lucru este valabil și în cazul supravegherii prin mijloace de comunicații electronice, dată fiind utilizarea extrem de largă a acestora în cadrul relațiilor de serviciu (spre ex: e-mail, fax, comunicator, messenger etc.)

- comunicarea prin mijloace electronice este esențială și extrem de uzuală în derularea normală a relațiilor de muncă, astfel încât supravegherea acestora de către angajator reprezintă o exercitare normală a prerogativei sale de organizare și control, unul dintre principalele drepturi ale sale prevăzute de art. 40 lit. d) C. muncii
- este absolut rezonabil ca angajatorul să monitorizeze e-mail-urile cu conținut legat de activitatea profesională, precum și orice alte comunicări de această natură prin diverse alte mijloace de comunicare electronică; în caz contrar,
- prin impunerea acestor condiții drastice legate de supraveghere (doar în caz de activități deosebite, stocare maxim 30

			de zile) dreptul său de a supraveghea activitatea angajaților este extrem de limitat, fiind aproape golit de conținut • însăși CEDO, în cauza Bărbulescu, a făcut distincție între supravegherea prin mijloace electronice în ceea ce privește activitatea desfășurată cu titlu profesional și cea de natură privată (făcând distincția între contul de serviciu și cel personal), apreciind că supravegherea comunicațiilor electronice legate de activitatea profesională este perfect admisibilă, neafectând dreptul la viață privată al salariaților • or, în cazul de față, art. 5 nu face distincția între supravegherea comunicațiilor electronice în legătură cu activitatea de serviciu și cele legate de viața privată a angajatului
4.	ART. 11 Aplicarea masurilor corective autoritatilor și organismelor publice Pentru încălcarea prevederilor Regulamentului general privind protecția datelor și ale prezentei legi de către autoritățile și organismele publice, Autoritatea Națională de supraveghere poate lua măsurile coercitive prevăzute de art 58 alin (2) lit a)-h) și lit j) din Regulamentul general privind protecția datelor.	ART. 11 Aplicarea masurilor corective autoritatilor și organismelor publice Pentru încălcarea prevederilor Regulamentului general privind protecția datelor și ale prezentei legi de către autoritățile și organismele publice și de către alți operatori de date cu caracter personal din domeniul public sau privat, Autoritatea Națională de supraveghere poate lua măsurile coercitive prevăzute de art 58 alin (2) lit a)-h) și lit j) din Regulamentul general privind protecția datelor.	Având în vedere scopurile urmărite de GDPR și abordarea mai restrictivă aplicată de acesta în multe cazuri prin raportare la procesările de date cu caracter personal efectuate de către autoritățile sau instituțiile publice nu considerăm oportună stabilirea unei răspunderi cu caracter derogatoriu, mai puțin severă ca și nivel al potențialelor sancțiuni tocmai pentru aceste entități. În acest context o abordare echitabilă constă în aplicarea unui regim sancționatoriu comun tuturor jucătorilor din acest domeniu. <i>Pentru cazul operatorilor din domeniul privat</i>

			<i>putem sustine aplicarea cuantumului amenzilor propus (diminuat fata de prevederile Regulamentului) pe durata a 3 (trei) ani de la intrarea în viitoare a legii.</i>
5.	ART. 12 – Constatarea contravențiilor și aplicarea de sancțiuni autorităților și organismelor publice (1) în funcție de circumstanțele fiecărui caz în parte, Autoritatea Națională de Supraveghere poate impune mustrare sau amendă. Amendă se stabilește în conformitate cu articolul 83 din Regulamentul general privind protecția datelor și în baza criteriilor prevăzute de art 83 alin. 2 din același regulament. (2) Constituie contravenție, fapta de încălcare de către autoritățile și organismele publice, a următoarelor dispoziții din Regulamentul general privind protecția datelor referitoare la: (...) (3) Constituie contravenție fapta de încălcare, de către autoritățile și organismele publice, a dispozițiilor art. 3-7 din prezenta lege. (5) Constituie contravenție fapta de încălcare, de către autoritățile și organismele publice, a următoarelor dispoziții din Regulamentul general privind protecția datelor, referitoare	ART. 12 – Constatarea contravențiilor și aplicarea de sancțiuni autorităților și organismelor publice (1) în funcție de circumstanțele fiecărui caz în parte, Autoritatea Națională de Supraveghere poate impune mustrare sau amendă. Amendă se stabilește în conformitate cu articolul 83 în baza criteriilor prevăzute de art 83 alin. 2 din același regulament. (2) Constituie contravenție, fapta de încălcare de către autoritățile și organismele publice și de către alți operatori de date cu caracter personal din domeniul public sau privat, a următoarelor dispoziții din Regulamentul general privind protecția datelor referitoare la: (...) 3) Constituie contravenție fapta de încălcare, de către autoritățile și organismele publice și de către alți operatori de date cu caracter personal din domeniul public sau privat, a dispozițiilor art. 3-7 din prezenta lege (5) Constituie contravenție fapta de încălcare, de către autoritățile și organismele publice și de către alți operatori de date cu caracter personal din domeniul public sau privat, a următoarelor dispoziții din Regulamentul	Eliminarea sintagmei « în conformitate cu articolul 83-» în vederea corelării acestui punct cu următoarele mențiuni ale articolului referitoare la cuantumul sancțiunilor. Având în vedere scopurile urmărite de Regulamentul general de protecție a datelor și abordarea mai restrictivă aplicată de acesta în multe cazuri prin raportare la procesările de date cu caracter personal efectuate de către autoritățile sau instituțiile publice nu considerăm oportună stabilirea unei răspunderi cu caracter derogatoriu, mai laxă ca și nivel al potențialelor sancțiuni tocmai pentru aceste entități. În acest context o abordare echitabilă constă în aplicarea unui regim sancționatoriu comun tuturor jucătorilor din acest domeniu.

	la:.... (7) Constituie contravenție fapta de încălcare de către autoritățile și organismele publice a unei decizii emise de Autoritatea Natională de Supraveghere a Prelucrării Datelor în conformitate cu art 58 alin(2) coroborat cu art 83 alin(2) din Regulamentul general privind protecția datelor.	general privind protecția datelor, referitoare la:.... (7) Constituie contravenție fapta de încălcare de către autoritățile și organismele publice și de către alți operatori de date cu caracter personal din domeniul public sau privat, a unei decizii emise de Autoritatea Natională de Supraveghere a Prelucrării Datelor în conformitate cu art 58 alin(2) coroborat cu art 83 alin(2) din Regulamentul general privind protecția datelor. (8) Contravențiile prevăzute de prezenta lege și de Regulamentul general privind protecția datelor intră sub incidența Legii prevenirii nr. 270/2017. (9) În cazul nerespectării planului de remediere, prevăzut de Legea prevenirii nr. 270/2017, amenda aplicată contravențiilor prevăzute de prezenta lege și Regulamentul general privind protecția datelor va putea fi investită de către contravenient în aducerea la conformitate a încălcărilor constatate prin procesul verbal de constatare a contravenției. Contravenientul va avea obligația de a proba investițiile.	
6.	Cap. VII – Dispoziții tranzitorii și finale Art.13 (1) Dispozițiile Regulamentului general privind protecția datelor se aplică plangerilor și sesizărilor depuse și înregistrate la Autoritatea Natională de Supraveghere începând cu data aplicării	Cap. VII – Dispoziții tranzitorii și finale Art.13 (1) Dispozițiile Regulamentului se aplică plangerilor și sesizărilor depuse și înregistrate la Autoritatea natională de supraveghere, precum și celor depuse înainte de 25 mai 2018 și aflate în curs de soluționare. Investigatiile efectuate pentru	Având în vedere următoarele: a) impactul semnificativ al aplicării prevederilor Regulamentului general b) efortul pentru implementarea acestuia la nivelul tuturor entităților care activează la nivelul țării noastre, Apreciem că se impune stabilirea unei perioade de tranziție și efectuare a demersurilor necesare conformării. Astfel, sub aspectul sancțiunilor prevăzute de Regulamentul general, susținem că acestea să fie supuse prevederilor Legii prevenirii nr. 270/2017. Având în vedere faptul că Regulamentul a intrat în vigoare în data de 25 mai 2016 dar va fi aplicabil începând din 25 mai 2018, Articolul 13 nu este foarte clar cu privire la legea aplicabilă și regimul sancționator pentru faptele săvârșite anterior aplicării Regulamentului. Atunci când se menționează “acte normative în

acestui, precum și celor depuse înainte de 25 mai 2018 și aflate în curs de soluționare. Investigatiile efectuate pentru soluționarea acestora și investigatiile din oficiu, începute anterior datei de 25 mai 2018 și nefinalizate la aceasta dată, sunt supuse dispozițiilor aceluiași regulament. (2) Constatarea faptelor și aplicarea măsurilor coercitive, inclusiv a sancțiunilor contravenționale, după data de 25 mai 2018, se realizează în conformitate cu prevederile Regulamentului general privind protecția datelor, ale Legii 102/ 2005 și ale prezentei legi. (3) În cazul în care Regulamentul general privind protecția datelor și prezenta lege prevăd o sancțiune mai gravă, contravenția săvârșită anterior datei de 25 mai 2018 va fi sancționată conform dispozițiilor actelor normative în vigoare la data săvârșirii acesteia. În situațiile în care, potrivit Regulamentului general privind protecția datelor și prezentei legi, fapta nu mai este considerată contravenție, aceasta nu se sancționează, chiar dacă a fost săvârșită înainte de data de 25 mai 2018.	soluționarea acestora și investigatiile din oficiu începute anterior datei de 25 mai 2018 și nefinalizate la aceasta dată, sunt supuse dispozițiilor aceluiași regulament. începând cu data aplicării acestuia. (2) Constatarea faptelor și aplicarea sancțiunilor coercitive inclusiv a sancțiunilor contravenționale, după data de 25 mai 2018, se realizează în conformitate cu prevederile Regulamentului general privind protecția datelor, ale Legii 102/ 2005 și ale prezentei legi. pentru fapte săvârșite ulterior datei de aplicare a Regulament va fi supusă sancțiunilor prevăzute de Regulament. (3) În cazul în care Regulamentul general privind protecția datelor și prezenta lege prevăd o sancțiune mai gravă, contravenția săvârșită anterior datei de 25 mai 2018 va fi sancționată conform dispozițiilor actelor normative în vigoare la data săvârșirii acesteia. În situațiile în care, potrivit actelor normative aplicabile la data săvârșirii faptei sau potrivit Regulamentului general privind protecția datelor și prezentei legi, fapta nu constituie contravenție, aceasta nu se sancționează.	vigoare la data săvârșirii, se creează o confuzie, întrucât, pentru doi ani, în România au fost în vigoare atât Legea 677/ 2001, cât și Regulamentul. În considerarea faptului că Regulamentul devine aplicabil din 25 mai 2018, considerăm că acesta <u>nu poate fi aplicat retroactiv</u>, respectiv nu poate fi aplicat faptelor săvârșite anterior acestei date. În acest sens, faptele săvârșite anterior datei de 25 mai 2018, indiferent de momentul în care sunt depuse eventuale plângeri și sesizări sau sunt efectuate investigații, constatarea faptelor și aplicarea sancțiunilor trebuie să fie supuse Legii 677/ 2001. Faptele săvârșite după 25 mai 2018 sunt supuse Regulamentului. Pe de altă parte, articolul în forma aceasta poate ridica probleme în cazul contravențiilor continue (conform OG nr. 2/2001, "Contravenția este continuă în situația în care încălcarea obligației legale durează în timp", o prelucrare nelegitimă de date putând fi considerată o contravenție continuă. Din aceste considerente și în acest sens, am propus modificări ale Articolului 13 în vederea clarificării regimului normativ aplicabil faptelor în funcție de data săvârșirii lor, respectiv înainte de 25 mai 2018 și după această dată.
--	--	---

Observatii:

- este necesară reformularea definiției numărului de identificare național în sensul ca aceasta să cuprindă în sfera sa doar codul numeric personal și numărul de asigurare socială;
- art. 9 – Acreditarea organismelor de certificare, pct. (1), pare să sugereze că numai asociațiile acreditate de RENAR pot acorda certificari în România, ceea ce este foarte restrictiv, însemnând că o societate cu o certificare acordată de un organism din altă țară europeană trebuie să își mai ia o certificare și în România. Limitarea în cauză are caracter monopolist, anticoncurențial și poate duce la cazuri de abuz reglementar (regulatory abuse). Este necesară adăugarea unei prevederi explicative în sensul de a nu exclude certificările de la alte organisme naționale sau europene legal acreditate conform legilor din țările lor.