editorial

Guvernanţa datelor în 2025: Între conformitatea proactivă şi costurile neglijenţei

Data Governance in 2025: Between Proactive Compliance and the Costs of Negligence

Doru DOROBANŢU*

Pendulând între dezideratul protecţiei implicite şi severitatea sancţiunilor aplicate de autorităţi, anul 2025 a oferit o lecţie de realism juridic în managementul operaţiunilor de prelucrare a datelor cu caracter personal. Este şi motivul pentru care putem afirma, fără echivoc, că într-un mediu marcat de o efervescenţă digitală evidentă, protecţia vieţii private nu ar trebui să mai reprezinte o simplă bifă procedurală, ci să devină un standard de excelenţă şi un barometru al integrităţii organizaţionale.

Realitatea surprinsă de analiza incidentelor constatate de autorităţi, atât din ţară, cât şi din alte state europene, este una sobră: acolo unde inovaţia tehnică devansează rigoarea normativă, se constată o vulnerabilitate sistemică ce transformă progresul tehnologic într-o expunere juridică iminentă. Discrepanţa dintre entuziasmul tehnologic şi rigoarea administrativă rămâne principala sursă de risc.

Dacă luăm în considerare „peisajul" sancţiunilor aplicate în România, putem observa oglinda neglijenţei organizatorice.

Astfel, anul 2025 a fost marcat de o diversificare a sectoarelor investigate de ANSPDCP, de la instituţii de învăţământ şi administraţie publică, până la giganţi din sectorul bancar, retail şi energie.

O evaluare din prisma **vulnerabilităţilor în securitatea cibernetică** a cazurilor privind furnizorul de soluţii software NTT DATA România (amendă de aprox. 25.000 EUR) şi companiei BEKO România (amendă 10.000 EUR) subliniază o problemă cronică: absenţa testării periodice a securităţii sistemelor de prelucrare şi depăşirea termenului de notificare a breşelor (72 de ore), precum şi acces neautorizat la datele personale ale clienţilor, din cauza unor măsuri tehnice şi organizatorice inadecvate.

Atacurile de tip ransomware (ex: PGS Sofa & Co, Greencorp) au demonstrat că lipsa autentificării multi-factor (MFA) nu mai este doar o omisiune tehnică, ci o încălcare sancţionabilă a art. 32 GDPR, poate prea puţin sancţionată.

* Profesor asociat, Şcoala Naţională de Studii Politice şi Administrative.

Pe de altă parte, **supravegherea excesivă și nerespectarea drepturilor persoanelor vizate**/angajaților au fost aduse în atenție prin sancțiunile aplicate Liceului Vasile Conta (camere video în grupuri sanitare) și poliților locale din Miercurea Ciuc și Craiova (body-cam fără temei legal). Aceste cazuri, dar și multe altele asemenea, reiterează un o regulă care ar trebui să fie considerate principiu fundamental: tehnologia nu poate substitui legalitatea.

Este încă o dovadă că este prea puțin cunoscut că utilizarea mijloacelor audio-video necesită un temei juridic precis și o analiză de impact (DPIA) reală, nu formală.

Pentru segmentul de **E-commerce și Marketing Direct,** în ceea ce privește **drepturile persoanelor vizate de prelucrări,** operatori consacrați precum PPC Energie sau Lensa (Tensa Art Design) au fost sancționați pentru ignorarea dreptului de opoziție.

Mesajul Autorității a fost clar: marketingul „agresiv", bazat pe consimțământ viciat sau baze de date neactualizate, trebuie sancționat și poate că astfel generează costuri mult mai mari decât profitul imediat.

Dacă privim spre tendințele europene, observăm crearea unor precedente care redefinesc piața.

Nu putem să nu menționăm că, la nivel European, anul 2025 a adus amenzi uriașe și decizii care trasează noi linii de demarcație pentru companiile tech. Pe domenii precum **publicitatea targetată și giganții Tech,** se evidențiază menținerea amenzii de 746 milioane EUR pentru Amazon în Luxemburg și noile sancțiuni împotriva Google (325 mil. EUR) și SHEIN (150 mil. EUR) în Franța, fiind confirmat sfârșitul modelului „consimțământului implicit" pentru cookie-uri.

În situația **transferurilor transfrontaliere de date,** cazul TikTok (amendă de 530 milioane EUR în Irlanda) reprezintă un avertisment critic pentru orice entitate care transferă date către jurisdicții terțe (ex: China) fără garanții echivalente celor din UE. Astfel, transferul ilegal și nesigur al datelor personale ale utilizatorilor europeni în China, fără să ofere transparență și protecție adecvată, a determinat sancționarea companiei de către Comisia pentru Protecția Datelor din Irlanda.

Pe segmental în care este implicată **Inteligența Artificială (AI),** sancționarea chatbot-ului „Replika" în Italia evidențiază o altă problemă: protecția minorilor în interacțiunea cu algoritmii AI și necesitatea unui temei legal transparent pentru antrenarea modelelor. Autoritatea Italiană pentru Protecția Datelor a amendat cu 5 milioane de euro compania americană Luka Inc., dezvoltatoarea chatbotului „Replika", care permite utilizatorilor să creeze un „însoțitor virtual" cu rol de confident, terapeut, partener romantic sau mentor. Nu trebuie să uităm că, încă din 2024, Autoritatea Olandeză pentru Protecția Datelor a tras un semnal de alarmă cu privire la riscurile utilizării unui chatbot bazat pe AI, atunci când au fost împărtășite date cu caracter personal ale unor pacienți sau clienți cu o astfel de tehnologie.

Utilizarea asistenților digitali, precum ChatGPT, Claude, Cursor sau Copilot, pentru a răspunde întrebărilor clienților sau pentru a rezuma fișiere voluminoase poate părea tentantă, din perspectiva economisirii timpului. Cu toate acestea, această practică implică riscuri semnificative pentru confidențialitatea datelor.

Așadar, ce lecții putem învăța până acum din anul 2025?

Voi evidenția doar patru aspecte critice pe care orice operator trebuie să le adreseze pentru a evita vulnerabilitatea structurală:

1. **Cultura responsabilității:** cazurile în care angajații divulgă date pe rețelele sociale demonstrează că investiția în firewall-uri este inutilă fără o un proces constant de instruire a factorului uman.

2. **Ieşirea din „amnezia" securităţii:** notificarea incidentelor fără întârzieri nejustificate, în cel mult 72 de ore nu este opţională. Totodată, lipsa procedurilor de revocare a accesului la date şi sisteme de prelucrare pentru foştii angajaţi rămâne o breşă de securitate elementară şi de cele mai multe ori extrem de costisitoare.

3. **Transparenţa cookie-urilor:** simpla existenţă a unui banner de informare nu asigură conformitatea. Utilizatorul trebuie să aibă o opţiune reală de refuz, fără a fi constrâns sau dezinformat.

4. **DPIA ca instrument de management, nu document de sertar:** Atât în cazul spitalelor, cât şi al magazinelor (cazul **Samaritaine**), absenţa unei Evaluări de Impact înainte de instalarea sistemelor de monitorizare a condus direct la sancţiuni.

În concluzie, în zilele noastre o strategie bazată pe „nu o să mi se întâmple tocmai mie" nu mai poate fi o strategie de business. Diferenţa dintre un operator rezilient şi unul vulnerabil rezidă în capacitatea de a demonstra responsabilitate, dar acea responsabilitate înţeleasă în sensul englezescului *accountability*, adică să fii responsabil şi să poţi face oricând dovada responsabilităţii tale.

Trebuie să o spunem deschis, GDPR nu pretinde perfecţiune tehnică, ci control real, transparenţă şi respect faţă de persoana vizată.

Într-o lume în care datele sunt „noul petrol", încrederea utilizatorului este singura monedă care nu se devalorizează. Proiectele operatorilor care reuşesc să armonizeze performanţa cu protecţia datelor încă din faza de design sunt singurele care vor transforma inovaţia într-un avantaj competitiv sustenabil.

Digital Omnibus: între promisiunea simplificării şi erodarea protecţiei datelor în Uniunea Europeană

Digital Omnibus: between the promise of simplification and the erosion of data protection in the European Union

Raluca Anica ONUFREICIUC*
Alin TOMUŞ**

❑ **Rezumat**

În cadrul acestui articol ne propunem să analizăm pachetul „Digital Omnibus" prezentat de Comisia Europeană în noiembrie 2025, evaluând tensiunea dintre obiectivul declarat de simplificare a conformării şi riscul de diminuare a standardelor de protecţie a datelor în Uniunea Europeană. Sunt examinate, în principal, amendamentele propuse la Regulamentul RGDP şi repoziţionarea regimului ePrivacy, cu accent pe: restrângerea noţiunii de „date cu caracter personal" prin criteriul „mijloacelor rezonabile" ale operatorului; instituţionalizarea unor mecanisme de adaptare la evoluţiile tehnice privind pseudonimizarea; extinderea utilizării interesului legitim pentru antrenarea, testarea şi validarea sistemelor de inteligenţă artificială; flexibilizarea regimului cererilor de acces şi lărgirea excepţiilor de la obligaţiile de transparenţă. De asemenea, analiza normativa vizează şi aspect legate de modernizarea consimţământului pentru cookie-uri (prin excepţii suplimentare şi semnale de consimţământ „machine-readable"), armonizarea raportării incidentelor printr-un punct unic şi ajustările propuse AI Act (inclusiv derogări limitate privind datele sensibile pentru mitigarea bias-ului şi reconfigurarea calendarului de conformare). În concluzie susţinem că, deşi pachetul poate reduce costurile de conformare şi fragmentarea obligaţiilor, anumite reforme riscă să producă o „simplificare" asimetrică, în beneficiul operatorilor şi în detrimentul garanţiilor materiale, reclamând limitări şi condiţii mai stricte în procesul legislativ pentru menţinerea nivelului de protecţie impus de Carta drepturilor fundamentale a Uniunii Europene.

* Avocat Doctorand la Universitatea Nicolae Titulescu din Bucureşti şi Universitatea Paris-Panthéon-Assas, asist. univ. drd., Universitatea „Ştefan cel Mare" din Suceava, Facultatea de Drept şi Ştiinţe Administrative, e-mail: raluca.onufreiciuc@fdsa.usv.ro.

** Dr., Membru al Centrului Interdisciplinar de cercetare în dreptul concurenţei, transformărilor digitale şi noilor tehnologii (CCTD), Universitatea „Ştefan cel Mare" din Suceava, e-mail: alintomus@gmail.com.

Cuvinte-cheie: *Digital Omnibus; reforma GDPR; ePrivacy; simplificarea conformării; AI Act; consimţământ pentru cookie-uri; drepturile persoanelor vizate; reglementarea digitală a UE.*

❑ Abstract

This article critically analyses the Digital Omnibus package presented by the European Commission in November 2025, assessing the tension between the declared objective of simplifying compliance and the risk of weakening data protection standards in the European Union. It primarily examines the proposed amendments to the GDPR and the repositioning of the ePrivacy regime, with a focus on: the narrowing of the concept of „personal data" through the criterion of the controller's „reasonable means"; the institutionalisation of mechanisms designed to adapt the GDPR to technological developments in pseudonymisation; the expanded reliance on legitimate interests for the training, testing, and validation of artificial intelligence systems; the flexibilisation of the regime governing data subject access requests (DSARs); and the broadening of exemptions from transparency obligations. In parallel, the article discusses the modernisation of cookie consent (through additional exceptions and machine-readable consent signals), the harmonisation of incident reporting via a single-entry point, and the proposed adjustments to the AI Act (including limited derogations concerning the use of sensitive data for bias mitigation and the reconfiguration of compliance timelines). As a first conclusion, we noticed that while the package may reduce compliance costs and regulatory fragmentation, certain reforms risk producing an asymmetric form of „simplification" that benefits controllers at the expense of substantive safeguards, thereby calling for stricter limitations and conditionalities in the legislative process to preserve the level of protection required by the European Union Charter of Fundamental Rights.

Keywords: *Digital Omnibus; GDPR reform; ePrivacy; compliance simplification; AI Act; cookie consent; data subjects' rights; EU digital regulation.*

1. Introducere

În data de 19 noiembrie 2025, Comisia Europeană a prezentat pachetul legislativ „Digital Omnibus", o inițiativă amplă[1] menită să simplifice și să eficientizeze cadrul de reglementare digital al Uniunii Europene.

Deși la nivel declarativ propunerile reprezintă un set de amendamente tehnice menite să reducă povara administrativă și costurile conformării, stimulând competitivitatea afacerilor, în realitate pachetul redeschide spre revizuire unele dintre principalele acte normative în materia protecției datelor și vieții private – inclusiv Regulamentul RGDP[2] și Directiva ePrivacy[3], fapt surprinzător și intens criticat de

[1] Comisia Europeană, *Propunere de regulament al Parlamentului European și al Consiliului de modificare a Regulamentelor (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 și a Directivelor 2002/58/CE, (UE) 2022/2555 și (UE) 2022/2557 în ceea ce privește simplificarea cadrului legislativ digital și de abrogare a Regulamentelor (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 și a Directivei (UE) 2019/1024* (Digital Omnibus), COM(2025) 837 final, 2025/0360 (COD), Bruxelles, 19 noiembrie 2025, https://digital-strategy.ec.europa.eu/ro/library/digital-omnibus-regulation-proposal.

[2] Regulamentul (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 privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE

organizaţiile pentru drepturile digitale şi de specialiştii în protecţia datelor, care au avertizat că noile modificări ar putea submina drepturi fundamentale ale persoanelor şi garanţii esenţiale prevăzute de cadrul juridic actual.

Pe lângă propunerile de modificare a principalelor acte legislative din domeniul digital, acesta cuprinde şi instituirea unui „European Business Wallet" (un portofel electronic european pentru companii) şi impulsionarea unei strategii pentru o Uniune Europeană a Datelor. Comisia prezintă aceste propuneri drept o recalibrare strategică a cadrului de reglementare digital al UE, considerat ca având nevoie de simplificare, o mai bună coordonare şi eficienţă sporită, aducând amendamente punctuale la câteva acte normative esenţiale cu impact direct asupra sectorului privat care operează în spaţiul european (Regulamentul RGDP, Directiva ePrivacy, Legea privind inteligenţa artificială[1] (*AI Act*), Legea datelor[2] (*Data Act*), precum şi norme privind raportarea incidentelor cibernetice în temeiul diferitelor reglementări (*eg*. DORA[3], NIS2[4]).

Scopul general al Digital Omnibus este de a reduce sarcinile administrative[5] şi suprapunerile legislative existente, de a îmbunătăţi coerenţa şi claritatea normelor digitale şi de a stimula inovaţia şi competitivitatea în economia digitală europeană[6].

La nivel instituţional şi juridic, propunerile Digital Omnibus se înscriu în eforturile mai largi ale UE de a actualiza şi recalibra acquis-ul digital. În ultimul deceniu, Uniunea Europeană a adoptat numeroase reglementări majore în domeniu – de la RGPD (aplicabil din 2018) la acte normative recente precum *Digital Services Act* (DSA[7]) şi

(Regulamentul general privind protecţia datelor – RGDP), Jurnalul Oficial al Uniunii Europene L 119, 4 mai 2016.

[3] Parlamentul European şi Consiliul Uniunii Europene. *Directiva 2002/58/CE din 12 iulie 2002 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice (Directiva privind confidenţialitatea şi comunicaţiile electronice – ePrivacy).* Jurnalul Oficial al Uniunii Europene L 201, 31 iulie 2002, cu modificările ulterioare.

[1] Regulamentul (UE) 2024/1689 al Parlamentului European şi al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligenţa artificială (Legea privind inteligenţa artificială – AI Act). Jurnalul Oficial al Uniunii Europene L, 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

[2] Regulamentul (UE) 2023/2854 al Parlamentului European şi al Consiliului din 13 decembrie 2023 privind normele armonizate pentru accesul echitabil la date şi utilizarea acestora (Data Act). Jurnalul Oficial al Uniunii Europene L, 22 decembrie 2023.

[3] Regulamentul (UE) 2022/2554 al Parlamentului European şi al Consiliului din 14 decembrie 2022 privind *rezilienţa operaţională digitală a sectorului financiar* (DORA), Jurnalul Oficial al Uniunii Europene L, 2022.

[4] Comisia Europeană, *Directiva (UE) 2022/2555 a Parlamentului European şi a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune şi de abrogare a Directivei (UE) 2016/1148 (NIS2)*, Jurnalul Oficial al Uniunii Europene L 333, 27 decembrie 2022, https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

[5] V. Wellens, O. Covolo, J. Van Overbeke, „Simplification of EU digital regulations: The Digital Omnibus", *NautaDutilh*, 17 decembrie 2025, https://www.nautadutilh.com/en/insights/simplification-of-eu-digital-regulations-the-digital-omnibus/.

[6] B. Martens, „The European Union needs more than the digital omnibus to make digital services competitive", *Analysis*, Bruegel, 8 decembrie 2025, https://doi.org/10.64153/NIRG1605.

[7] Regulamentul (UE) 2022/2065 al Parlamentului European şi al Consiliului din 19 octombrie 2022 privind o piaţă unică pentru serviciile digitale şi de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale – Digital Services Act), JO L 277, 27 octombrie 2022, 1-102.

Digital Markets Act (DMA[1]) – ceea ce a dus la un cadru complex, cu obligaţii uneori suprapuse (de exemplu, cerinţe de raportare a incidentelor) şi costuri administrative ridicate pentru organizaţii. Comisia Europeană, urmărind obiectivul general de a reduce povara administrativă cu 25% (şi cu 35% pentru IMM-uri până în 2029), a iniţiat totodată o amplă evaluare a coerenţei legislaţiei digitale existente (aşa-numitul *Digital Fitness Check*[2], deschis până în martie 2026) pentru a identifica disfuncţionalităţile şi sarcinile inutile. În acest context, propunerea de regulament a Omnibus-ului digital vine să ajusteze punctual cadrul normativ, eliminând incoerenţele şi redundanţele, consolidând piaţa unică digitală (inclusiv prin instrumente noi de identitate electronică, precum *European Business Wallet*) şi astfel să creeze un mediu legislativ[3] mai previzibil şi mai uşor de administrat. Propunerile Comisiei reprezintă doar prima etapă a procesului legislativ: ele urmează să fie dezbătute şi eventual modificate de Parlamentul European şi Consiliu în cursul procedurii de co-decizie, înainte de a intra în vigoare.

2. Analiza principalelor modificări propuse prin pachetul Digital Omnibus

Un prim set de modificări vizează Regulamentul RGPD şi regulile de confidenţialitate în comunicaţii electronice, şi anume se propune *redefinirea sferei datelor cu caracter personal*[4] - informaţiile care nu pot fi atribuite unei persoane identificate sau identificabile prin mijloace rezonabile aflate la dispoziţia operatorului nu ar mai fi considerate date personale, ceea ce restrânge domeniul de aplicare al regulamentului. În

[1] Regulamentul (UE) 2022/1925 al Parlamentului European şi al Consiliului din 14 septembrie 2022 privind pieţe contestabile şi echitabile în sectorul digital şi de modificare a Directivelor (UE) 2019/1937 şi (UE) 2020/1828 (Regulamentul privind pieţele digitale) (Text cu relevanţă pentru SEE), JO L 265,12 octombrie 2022, 1-66.

[2] Comisia Europeană, *Digital Fitness Check: testarea impactului cumulativ al normelor digitale ale Uniunii Europene*, iniţiativă de tip „call for evidence" şi consultare publică, Bruxelles, 19 noiembrie 2025, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/15554-Digital-fitness-check-testing-the-cumulative-impact-of-the-EUs-digital-rules_en.

[3] MedTech Europe, *„MedTech Europe's input to the Digital Simplification Package consultation"*, 6 noiembrie 2025, accesat 23 decembrie 2025, https://www.medtecheurope.org/2025/11/06/digital-omnibus/.

[4] Textul propus: *(1) „date cu caracter personal" înseamnă orice informaţii referitoare la o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un identificator precum un nume, un număr de identificare, date de localizare, un identificator online sau la unul ori mai mulţi factori specifici identităţii fizice, fiziologice, genetice, psihice, economice, culturale sau sociale a respectivei persoane fizice.*

Informaţiile referitoare la o persoană fizică nu sunt neapărat date cu caracter personal pentru orice altă persoană sau entitate, doar pentru faptul că o altă entitate poate identifica acea persoană fizică. Informaţiile nu sunt date cu caracter personal pentru o anumită entitate atunci când acea entitate nu poate identifica persoana fizică la care se referă informaţiile, ţinând seama de mijloacele care sunt, în mod rezonabil, susceptibile de a fi utilizate de respectiva entitate. Astfel de informaţii nu devin date cu caracter personal pentru acea entitate doar pentru faptul că un potenţial destinatar ulterior dispune de mijloace care sunt, în mod rezonabil, susceptibile de a fi utilizate pentru a identifica persoana fizică la care se referă informaţiile.

plus, se instituie un mecanism de actualizare tehnologică[1] a pseudonimizării (un nou art. 41a Regulament RGPD) pentru a ține pasul cu evoluția tehnologică și noile tehnici de anonimizare a datelor. Alte modificări urmăresc *reducerea sarcinilor de conformare*: de exemplu, operatorii vor putea refuza sau taxa cererile abuzive ale persoanelor vizate (dreptul de acces) dacă acestea sunt „vădit nefondate sau excesive", ceea ce va ușura povara administrativă și probațiunea în caz de solicitări repetitive nejustificate. Se extind, de asemenea, excepțiile de la obligațiile de transparență: nu va mai fi necesar ca operatorul să furnizeze din nou informarea către persoana vizată dacă se poate prezuma că aceasta deține deja informațiile respective. În materie de securitate a datelor, notificarea autorităților în caz de încălcare (*breach*) va fi cerută numai pentru incidentele critice, termenul legal fiind prelungit de la 72 la 96 de ore – măsură menită să scutească firmele și autoritățile de notificări inutile pentru incidente minore. Nu în ultimul rând, regimul de cookies va suferi modificări importante[2]: se propune transferarea regulilor privind accesul la informația din terminalul utilizatorului din Directiva ePrivacy direct în RGPD, *sporind excepțiile de la consimțământ*[3] pentru utilizarea cookie-urilor.

Concret, un nou art. 88a RGPD ar permite prelucrarea datelor prin cookie-uri fără consimțământ în situații considerate necesare – de exemplu, pentru măsurarea audienței de către editorul unui site, pentru asigurarea securității serviciului sau pentru furnizarea unui serviciu online solicitat explicit de utilizator. Totodată, pachetul introduce obligativitatea respectării setărilor de confidențialitate exprimate de utilizator la nivelul dispozitivului sau al browser-ului (așa-numitele *semnale de consimțământ în format digital standardizat*), odată ce vor exista standarde tehnice în acest sens. Această măsură are drept scop diminuarea fenomenului de „*consent fatigue*" – reducând dependența de afișarea constantă a bannerelor de cookie – și transferarea controlului către utilizator prin preferințe automate care trebuie recunoscute și aplicate în mod obligatoriu de operatori.

Un al doilea set de modificări privește AI Act, care este ajustat în sensul creșterii *flexibilității și a caracterului favorabil inovației*. Se clarifică în primul rând relația cu RGPD: Comisia confirmă că prelucrarea de date personale pentru dezvoltarea și antrenarea algoritmilor de IA poate fi considerată legală în temeiul interesului legitim al operatorilor (art. 6(1) lit. f RGPD), cu condiția respectării garanțiilor existente (transparență față de persoanele vizate, minimizarea datelor, drept de opoziție etc.). Totodată, se introduce o excepție pentru folosirea datelor sensibile (cum ar fi date privind origine etnică, opinii politice, sănătate, ș.a., protejate de art. 9 RGPD) *exclusiv* în scopul detectării și corectării prejudecăților algoritmice din sistemele de IA. Această derogare recunoaște că, pentru a evalua și îmbunătăți echitatea și nediscriminarea algoritmilor, poate fi necesară referirea la astfel de date protejate, însă impune ca utilizarea lor să fie strict proporțională, limitată la acest scop și însoțită de măsuri de protecție adecvate, nefiind permisă pentru alte întrebuințări. Un alt aspect esențial este *amânarea și fazarea obligațiilor* din AI Act pentru sistemele IA cu risc ridicat (cele catalogate astfel în anexele regulamentului).

---

[1] Sophie Stalla-Bourdillon, *«Déjà vu in data protection law: the risks of rewriting what counts as personal data»*, *Privacy and Data Protection* 26, nr. 2 (1 decembrie 2025), pp. 9-10.

[2] NNDKP, *„European Commission launches the Digital Omnibus Proposal"*, *Privacy Out Loud*, 20 noiembrie 2025, https://privacyoutloud.ro/2025/11/20/european-commission-launches-the-digital-omnibus-proposal-2/.

[3] Noyb Report, *„Digital Omnibus: First Analysis of Select GDPR and ePrivacy Proposals by the Commission"*, 1 decembrie 2025, noyb.eu, https://noyb.eu/en/digital-omnibus-first-analysis-select-gdpr-and-eprivacy-proposals-commission/.

În loc ca cerinţele de conformare să intre automat în vigoare la o dată fixă după adoptarea actului, Digital Omnibus[1] prevede că acestea vor deveni aplicabile doar după ce Comisia Europeană confirmă că există suficiente standarde armonizate, orientări tehnice şi instrumente de suport pentru implementare. Cu toate acestea, sunt păstrate termene finale („*longstop deadlines*") până la care conformarea devine oricum obligatorie: de exemplu, sistemele din Anexa III a AI Act ar trebui să fie conforme până în decembrie 2027, iar cele din Anexa I până în august 2028. În plus, pentru a ţine cont de ritmul progresului tehnologic, se introduce o perioadă de graţie: furnizorii de sisteme de IA generativă puse pe piaţă înainte de august 2026 vor avea încă şase luni în plus pentru a se conforma cerinţelor de transparenţă (cum ar fi filigranarea conţinutului generat de AI şi etichetarea acestuia ca atare), dat fiind că standardele tehnice necesare pentru aceste obligaţii nu sunt încă finalizate. Măsurile propuse adresează şi *simplificarea cerinţelor administrative* din AI Act: se elimină obligaţia de a înregistra oficial în baza de date publică acele sisteme de IA care sunt folosite în medii cu risc ridicat, dar nu sunt ele însele clasificate ca având risc ridicat (rămânând doar necesitatea ca operatorul să documenteze intern evaluarea riscurilor acelui sistem). De asemenea, rolul Oficiului UE pentru IA este extins – această autoritate centrală (prevăzută de proiectul AI Act) va deveni competentă exclusiv pentru supravegherea sistemelor de IA bazate pe modele generale (inclusiv *foundation models* utilizate pe scară largă) şi a sistemelor de IA operate de platforme online foarte mari şi motoare de căutare (categoria VLOP/VLOSE definită de DSA). Această centralizare[2] urmăreşte asigurarea unei aplicări unitare a regulilor în toate statele membre, evitând fragmentarea supravegherii. Tot pentru eficientizare, procedurile de evaluare a conformităţii sistemelor IA vor fi unificate: organismele certificate vor putea obţine autorizarea printr-o singură procedură de notificare, valabilă atât pentru AI Act, cât şi pentru alte legislaţii de armonizare relevante, evitându-se duplicarea eforturilor. În ceea ce priveşte monitorizarea post-piaţă a sistemelor de IA, se propune eliminarea obligativităţii[3] utilizării unui format-tip impus de Comisie pentru planul de monitorizare – furnizorii îşi vor putea stabili propriile metode de urmărire a performanţei şi conformităţii sistemelor, ghidaţi de recomandările (neobligatorii) ale Comisiei, în locul unor formulare standard, ceea ce le conferă o mai mare flexibilitate operaţională. Nu în ultimul rând, pachetul extinde măsurile de clemenţă şi sprijin pentru IMM-uri prevăzute de AI Act: facilităţile de conformare simplificată care iniţial erau rezervate doar microîntreprinderilor se vor aplica tuturor IMM-urilor şi chiar *companiilor cu capitalizare medie* (mid-caps), de exemplu prin posibilitatea unor documentaţii mai simple, principii de sancţionare proporţională cu dimensiunea firmei şi ghiduri adaptate. În plus, conceptul de „sandbox" de reglementare

[1] ApTI, *„GDPR făcut ferfeniţă, sub numele Digital Omnibus"*, *Asociaţia pentru Tehnologie şi Internet*, 13 noiembrie 2025, https://www.apti.ro/content/GDPR-facut-ferfenita-sub-numele-digital-omnibus/.

[2] A&O Shearman (*Laurie-Anne Ancenys, Livio Bossotto, Dr. Catherine Di Lorenzo, Dr. Jens Matthes, Peter Van Dyck, Filip Van Elsen, Laur Badin, Nicole Wolters Ruckert, Justyna Ostrowska & Catharina Glugla*), *„Digital Omnibus Package: How will these changes affect your business?"*, Lexology, 25 noiembrie 2025, https://www.lexology.com/library/detail.aspx?g=5bd5b639-bff8-4fb1-ac94-a5b847b689d9.

[3] Stéphanie De Smedt, Virginie de France, Kirill Ryabtsev, Emilia Fronczak, Linde Vrolijk & Robert Fröger, *„Digital Omnibus: simplifying compliance and secure data identity management"*, Loyens & Loeff, 3 decembrie 2025, https://www.loyensloeff.com/insights/news-events/news/the---digital-omnibus-package-towards-simpler-digital-compliance-secure-data-use-and-unified-digital-identities-for-businesses/.

(mediu controlat de testare a inovaţiilor) este amplificat – Oficiul IA[1] va putea organiza un *sandbox* la nivelul întregii Uniuni pentru testarea în condiţii reale a sistemelor de IA[2] inovatoare (inclusiv a celor de IA cu scop general – *General Purpose AI*), iar statele membre vor putea stabili acorduri voluntare pentru a permite firmelor să realizeze teste transfrontaliere ale noilor soluţii de IA, extinzând astfel durata şi aria de aplicare a experimentelor desfăşurate dincolo de programele naţionale existente. Un sandbox european comun este deja prevăzut pentru anul 2028, în ideea asigurării unui cadru uniform de testare şi inovare sub supraveghere coordonată.

Un al treilea capitol al Digital Omnibus se concentrează pe regimul datelor în sens larg, vizând în principal *Data Act* şi legislaţia conexă referitoare la economia platformelor. Comisia propune o consolidare a normelor privind disponibilitatea şi partajarea datelor, prin contopirea mai multor instrumente juridice existente într-un cadru unic, integrat.

Printre actele care ar urma să fie unificate se numără Regulamentul privind guvernanţa datelor[3] (*Data Governance Act*), Regulamentul privind libera circulaţie a datelor nepersonale[4] (regulament din 2018) şi Directiva privind datele deschise[5] – aceste instrumente ar fi abrogate ca atare, iar dispoziţiile lor esenţiale ar fi preluate şi armonizate în textul Data Act, care ar suferi şi el modificări substanţiale.

Scopul este crearea unui cadru normativ unic al datelor, care să elimine inconsistenţele dintre diferitele legi şi să faciliteze sharing-ul de date între organizaţii, în condiţii de protecţie şi predictibilitate. În acest sens, Digital Omnibus aduce câteva clarificări cheie: redefineşte mai larg noţiunea de „deţinător de date" – acesta va fi orice persoană sau entitate care *ori utilizează, ori pune la dispoziţie date*, spre deosebire de definiţia actuală care impunea ambele obligaţii simultan. Se întăreşte, de asemenea, protecţia secretului comercial în contextul cererilor de acces la date: deţinătorii de date vor avea o marjă mai mare să refuze transferul de date solicitate de parteneri sau utilizatori, dacă divulgarea ar expune informaţii sensibile ori ar afecta interesele concurenţiale legitime ale acestora.

Un alt amendament extinde excepţiile de la regulile de portare şi interoperabilitate a serviciilor cloud în beneficiul furnizorilor de servicii de prelucrare a datelor personalizate, adică acele servicii create la comandă pentru nevoi specifice ale unui client şi care nu sunt oferite ca soluţii generice „de pe raft" (*off-the-shelf*). Pentru aceste servicii unicat, Data Act va permite clauze contractuale care să excludă obligaţia de portare sau interoperabilitate, recunoscând practic dificultatea de a schimba furnizorul

[1] M. Gartner, *„EU: First Analysis of the Digital Omnibus on AI"*, în *AIRe 4/2025 – Regulatory Pathways for AI: Europe, Asia, and the US*, AIRe – *Journal of AI Law and Regulation*, vol. 2, nr. 4/2025, p. 377, Lexxion Publisher, https://aire.lexxion.eu/article/AIRE/2025/4/10.

[2] BusinessEurope, *„Digital Omnibus proposals: An important milestone for EU competitiveness"*, 19 noiembrie 2025, https://www.businesseurope.eu/publications/digital-omnibus-proposal-an-important-milestone-for-eu-competitiveness/.

[3] Regulamentul (UE) 2022/868 al Parlamentului European şi al Consiliului din 30 mai 2022 privind guvernanţa europeană a datelor şi de modificare a Regulamentului (UE) 2018/1724 (Data Governance Act). *Jurnalul Oficial al Uniunii Europene* L 152, 3.6.2022.

[4] Regulamentul (UE) 2018/1807 al Parlamentului European şi al Consiliului din 14 noiembrie 2018 privind cadrul aplicabil liberei circulaţii a datelor nepersonale în Uniune. Jurnalul Oficial al Uniunii Europene L 303, 28.11.2018.

[5] Directiva (UE) 2019/1024 a Parlamentului European şi a Consiliului din 20 iunie 2019 privind datele deschise şi reutilizarea informaţiilor din sectorul public. Jurnalul Oficial al Uniunii Europene L 172, 26.6.2019.

unor servicii profund customizate. De asemenea, se prevede ca majoritatea obligaţiilor capitolului VI din Data Act (care reglementează schimbarea furnizorilor de servicii de prelucrare) să nu se aplice retroactiv contractelor încheiate înainte de 12 septembrie 2025, exceptând câteva obligaţii minimale – o măsură menită să protejeze acordurile existente de efectele noii legislaţii. În sfera platformelor online, Digital Omnibus[1] adresează suprapunerea normativă prin propunerea de abrogare a Regulamentului P2B (Platform-to-Business)[2].

Adoptat în 2019, acest regulament a fost primul pas în reglementarea echităţii relaţiilor dintre platformele online şi utilizatorii lor comerciali, însă de la 1 noiembrie 2022 au intrat în vigoare DSA) şi DMA, care acoperă mult mai cuprinzător şi detaliat problemele platformelor digitale. Comisia apreciază că DSA şi DMA au *depăşit în mare măsură* aria P2B, făcându-l parţial redundant. În consecinţă, se propune eliminarea acestuia, evitând dublarea obligaţiilor pentru platforme. Totuşi, planul prevede o perioadă de tranziţie până în 2032 şi menţinerea în vigoare, temporar, a anumitor dispoziţii P2B (probabil cele care nu sunt acoperite direct de DSA/DMA), astfel încât să nu existe lacune imediate.

De asemenea, Comisia indică faptul că Ghidul UE privind transparenţa algoritmilor de clasare (adoptat sub egida P2B) va rămâne un reper de referinţă chiar şi după abrogarea regulamentului, pentru a orienta bunele practici ale platformelor în asigurarea unui clasament corect şi transparent al produselor şi serviciilor. Per ansamblu, abrogarea P2B, combinată cu intrarea în vigoare a DSA/DMA, ar trebui să simplifice regimul juridic al platformelor online, reducând stratificarea normelor şi clarificând obligaţiile operatorilor din economia digitală.

3. Impactul „Digital Omnibus" asupra protecţiei datelor şi coerenţei cadrului juridic digital al UE

În scrisoarea transmisă[3] Comisiei Europene, organizaţiile European Digital Rights (EDRi), Irish Council for Civil Liberties (ICCL) şi noyb – European Center for Digital Rights îşi exprimă îngrijorarea că pachetul „Digital Omnibus" ar putea conduce la o dereglementare substanţială a cadrului juridic digital al Uniunii Europene, sub pretextul simplificării legislative. Autorii avertizează că modificările avute în vedere ar slăbi elemente esenţiale ale RGPD, ale cadrului e-Privacy şi ale AI Act, afectând protecţia

[1] M. Cornette, O. Haas, Dr. J. Hladjk, F. Mörth, M. Alexander Myers, M. Paez, L. Ropple şi Dr. Undine von Diemar, *„EU Digital Omnibus: How EU Data, Cyber, and AI Rules Will Shift"*, Jones Day, 19 decembrie 2025, https://www.jonesday.com/en/insights/2025/12/eu-digital-omnibus-how-eu-data-cyber-and-ai-rules-will-shift.

[2] Regulamentul (UE) 2019/1150 al Parlamentului European şi al Consiliului din 20 iunie 2019 privind promovarea echităţii şi a transparenţei pentru întreprinderile utilizatoare de servicii de intermediere online (Platform-to-Business – P2B). *Jurnalul Oficial al Uniunii Europene* L 186, 11.7.2019.

[3] A se vedea *Joint Letter: Digital Omnibus – Deregulation instead of simplification*, scrisoare comună adresată Comisiei Europene de European Digital Rights (EDRi), Irish Council for Civil Liberties (ICCL) şi noyb – European Center for Digital Rights, prin care sunt semnalate riscurile de diminuare a protecţiei drepturilor fundamentale şi de slăbire a cadrului GDPR, e-Privacy şi AI Act în contextul pachetului legislativ „Digital Omnibus, disponibilă la https://noyb.eu/en/open-letter-digital-omnibus-brings-deregulation-not-simplification.