DEPARTAMENTUL DE STUDII PARLAMENTARE ŞI POLITICI UE

DIRECŢIA STUDII ŞI DOCUMENTARE LEGISLATIVĂ

CREAREA ȘI UTILIZAREA CONTURILOR PE PLATFORME ONLINE – REGLEMENTĂRI, CONDIȚIONĂRI ȘI METODE DE IDENTIFICARE

studiu documentar

aprilie 2025

Documentare și sinteză: Aurora Trănescu
consilier parlamentar, Direcția studii și documentare legislativă
Palatul Parlamentului, str. Izvor nr.2-4, sect.5, București
Tel: 021.316.03.65; 021.414.13.50/ 51, Interior 1350/1349, camera 5070
E-mail: doc@cdep.ro

CUPRINS

INTRODUCERE

Regulamentul (UE) 2022/2065, cunoscut și sub denumirea de Regulamentul privind serviciile digitale (Digital Services Act - DSA), a fost adoptat la 19 octombrie 2022 și are ca obiectiv principal crearea unui cadru juridic uniform pentru serviciile digitale în Uniunea Europeană. Acesta vizează asigurarea unui mediu online sigur, previzibil și de încredere, prevenind diseminarea conținutului ilegal și protejând drepturile fundamentale ale utilizatorilor.

Regulamentul introduce obligații specifice pentru diferiți furnizori de servicii intermediare, inclusiv platforme online și rețele sociale. Aceste obligații includ măsuri de transparență, responsabilități în ceea ce privește moderarea conținutului și protecția consumatorilor. De asemenea, DSA armonizează normele aplicabile serviciilor intermediare pe piața internă, facilitând inovarea și asigurând respectarea drepturilor fundamentale.

Regulamentul (UE) 2022/2065 stipulează că Statele Membre trebuie să desemneze autoritățile competente pentru a fi responsabile cu supravegherea furnizorilor de servicii intermediare și asigurarea respectării actului legislativ. Aceste autorități competente poartă denumirea generică de coordonator pentru serviciile digitale, în limba engleză: *digital services coordinator* (DSC).

În România, Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM) a fost desemnată ca autoritate competentă responsabilă cu supravegherea furnizorilor de servicii intermediare și asigurarea respectării DSA. Regulamentul a intrat în vigoare la 16 noiembrie 2022 și se aplică începând cu 17 februarie 2024.

Regulamentul are aplicabilitate directă în statele membre UE. Mare parte dintre state au adoptat și propriile legi care pun în aplicare sau completează dispozițiile DSA și de regulă, în cadrul acestor legi sunt desemnate și instituțiile naționale cu rol de coordonator pentru serviciile digitale (DSC). Având în vedere aplicabilitatea directă, sunt de înțeles asemănările dintre modul de aplicare din diverse țări membre. Ca o excepție, amintim aici Spania și Polonia care nu au elaborat o legislație specifică, deși au existat discuții însă acestea nu s-au concretizat până în prezent.

Cerințele privind verificarea identității utilizatorilor pe platformele online variază în funcție de legislația fiecărui stat membru și de tipul serviciului oferit. În timp ce Regulamentul privind Serviciile Digitale (DSA) stabilește un cadru general pentru protecția utilizatorilor online, implementarea specifică a măsurilor de verificare a identității rămâne la latitudinea statelor membre.

Exemple de state membre cu cerințe specifice:

- Spania: a introdus cartera digital beta, o aplicație care stochează informații din actul de identitate național. Acesta este utilizat pentru a verifica în special vârsta utilizatorilor care accesează site-uri pentru adulți, asigurând astfel conformitatea cu restricțiile de vârstă.
- Italia: începând cu 2025, implementează Decretul Caivano, care impune utilizarea sistemului național de identitate digitală SPID pentru verificarea vârstei utilizatorilor ce accesează site-uri pornografice și de pariuri.
- Franța: a emis noi ghiduri care includ utilizarea recunoașterii faciale bazate pe inteligență artificială pentru estimarea vârstei utilizatorilor. Platformele care utilizează în prezent informații despre cardul de credit pentru verificarea vârstei au termen până în aprilie 2025 pentru a se conforma noilor norme.

La nivel european, se lucrează la dezvoltarea unui portofel digital european care să permită cetățenilor UE să se identifice online în condiții de siguranță și să acceseze servicii publice și private în întreaga Europă. Acest portofel digital este planificat să fie disponibil în 2026.

În concluzie, platformele online din diverse state UE pot solicita verificarea identității utilizatorilor în funcție de reglementările naționale și de tipul de servicii oferite, în special în domenii sensibile precum accesul la conținut pentru adulți sau servicii financiare.

Identificarea electronică, autentificare și servicii de încredere (Electronic Identification, Authentication, and Trust Services) – prescurtat eIDAS – este un regulament al Uniunii Europene (Regulamentul (UE) 910/2014) care stabilește un cadru pentru tranzacții electronice sigure în toate statele membre ale UE. Acesta garantează că identitățile digitale, semnăturile și serviciile de încredere sunt recunoscute din punct de vedere juridic și interoperabile în cadrul UE.

Comisia Europeană a inițiat proceduri de constatare a neîndeplinirii obligațiilor (*infringement*) împotriva mai multor state membre ale UE pentru punerea în aplicare necorespunzătoare a Digital Services Act (DSA). Toate țările UE au fost obligate să desemneze și să împuternicească un coordonator al serviciilor digitale (DSC) până la 17 februarie 2024. Când unele state membre nu au respectat acest termen, Comisia a inițiat proceduri privind încălcarea dreptului comunitar. Pentru că nu și-au desemnat DSC-urile la timp, prima rundă de scrisori de punere în întârziere a fost trimisă în iulie 2024 către: Franța, Italia, Polonia, Spania, Belgia, Bulgaria.
În decembrie 2024 a avut loc următoarea etapă a procesului, anume trimiterea avizelor motivate – sau scrisorile de punere în întârziere – către: Belgia, Bulgaria, Spania, Olanda, Polonia. De atunci, unele țări, cum ar fi Belgia, au luat măsuri prin desemnarea mai multor autorități competente pentru a-și îndeplini obligațiile.

În conformitate cu Regulamentul UE privind serviciile digitale (DSA), platformele online sunt supuse unui set de obligații pe niveluri, în funcție de mărimea și rolul lor. Menționăm aici defalcarea obligațiilor-cheie, pornind de la normele generale până la norme mai stricte pentru platformele online.

Obligații generale (pentru toți intermediarii online, inclusiv platformele):

- Gestionarea conținutului ilegal presupune că trebuie să acționeze prompt pentru a elimina conținutul ilegal atunci când este notificat și obligația de a pune la dispoziția utilizatorilor un mecanism de raportare a conținutului ilegal.
- Cerințe de transparență: informarea utilizatorilor atunci când conținutul este eliminat sau conturile sunt suspendate; publicarea de rapoarte de transparență privind acțiunile de moderare a conținutului.
- Claritatea condițiilor de utilizare: termenii și condițiile trebuie să fie clare, accesibile și ușor de înțeles.
- Trebuie să explice moderarea conținutului și procesele algoritmice.
- Obligații suplimentare pentru platformele online (de exemplu, piețe, social media): mecanisme de notificare și de acțiune: trebuie să permită utilizatorilor și părților terțe să notifice conținutul ilegal; trebuie să explice măsurile luate și să ofere o cale de atac.

- Sistem de reclamații și căi de atac: utilizatorii trebuie să aibă acces la un sistem intern de tratare a plângerilor; trebuie să fie disponibilă soluționarea extrajudiciară independentă a litigiilor.
- Semnalizatori de încredere (*trusted flaggers*): trebuie să se acorde prioritate notificărilor provenite de la persoanele desemnate ca semnalizatori de încredere.
- Transparență pentru publicitatea online: utilizatorii trebuie să poată vedea de ce le este afișată o anumită reclamă și cine a plătit pentru anunțul respectiv.
- Interzicerea modelelor obscure: interfețele nu pot manipula utilizatorii în luarea de decizii (de exemplu, prin design înșelător).

Platformele online foarte mari (VLOP) și motoarele de căutare online foarte mari (VLOSE) sunt platforme cu peste 45 de milioane de utilizatori din UE și se supun celor mai stricte reguli, inclusiv:

- evaluarea și diminuarea riscurilor sistemice;
- audituri independente anuale pentru verificarea conformității;
- accesul cercetătorilor la date;
- transparența sistemelor de recomandare: utilizatorii trebuie să fie informați cu privire la modul în care este recomandat conținutul, trebuie să ofere cel puțin o opțiune care nu se bazează pe profilare (de exemplu, flux cronologic).
- mecanisme de răspuns în caz de criză.

Mai jos prezentăm obligațiile cheie, conform Regulamentului (UE) 2022/2065 DSA, pentru cele mai mari platforme online active in Europa.

Amazon, piață online:

- trasabilitatea comercianților: trebuie să verifice și să divulge detaliile vânzătorilor terți pentru a proteja consumatorii („Know Your Business Customer”).
- listarea produselor ilegale: trebuie să răspundă prompt la notificările privind produsele ilegale sau nesigure.
- transparență algoritmică: trebuie să explice cum funcționează clasamentul și recomandările de produse, inclusiv influența anunțurilor sau a recenziilor.

- transparența anunțurilor: utilizatorii trebuie să vadă cine a plătit pentru o reclamă și de ce aceasta le este afișată.

De exemplu: dacă sunt raportate produse contrafăcute, Amazon trebuie să acționeze rapid, să informeze raportorul și să permită vânzătorilor să facă apel dacă produsul lor este eliminat.

TikTok, platformă social media / video de format scurt:

- transparența sistemului de recomandare: trebuie să explice modul în care funcționează pagina „Pentru dvs.” și să ofere o alternativă fără profilare (cum ar fi un feed cronologic);
- reducerea riscurilor sistemice: trebuie să evalueze și să reducă riscurile de: dezinformare, prejudicii aduse minorilor, provocări periculoase sau tendințe virale;
- moderarea conținutului: trebuie să explice clar orientările comunității și să notifice utilizatorii atunci când conținutul este eliminat;
- etichetarea anunțurilor: anunțurile trebuie să fie clar marcate, iar TikTok trebuie să dezvăluie criteriile de targetare a anunțurilor.

De exemplu: dacă tendințele dăunătoare sau informațiile eronate încep să devină virale, TikTok trebuie să evalueze riscurile și să pună în aplicare contramăsuri - cum ar fi reducerea reach-ului, adăugarea de avertismente sau promovarea informațiilor verificate.

Facebook (Meta), rețea socială/ platformă de distribuție de știri:

- atenuarea proactivă a riscurilor de dezinformare și manipulare politică;
- controlul sistemului de recomandare: trebuie să ofere mai mult control utilizatorului asupra fluxurilor (de exemplu, fluxuri de știri cronologice în loc de fluxuri bazate pe algoritmi);
- trebuie să acorde cercetătorilor autorizați acces la date privind răspândirea conținutului și dinamica platformei;
- restricții privind publicitatea targetată: în special în ceea ce privește datele sensibile (de exemplu, religia, opiniile politice).

De exemplu: în timpul alegerilor, Facebook trebuie să monitorizeze în mod activ manipularea sau anunțurile politice înșelătoare și să reacționeze rapid - toate acestea fiind în același timp transparente față de autoritățile de reglementare și utilizatori.

AUSTRIA

În Austria, punerea în aplicare a Regulamentului (UE) 2022/2065, cunoscut sub numele de Actul privind serviciile digitale (DSA), a fost formalizată prin DSA-Begleitgesetz (DSA-BegG)[1], care a intrat în vigoare la 30 decembrie 2023.

Acesta a introdus modificări ale legislației austriece existente pentru a asigura alinierea la dispozițiile DSA. Un aspect semnificativ a fost desemnarea Autorității austriece de reglementare pentru radiodifuziune și telecomunicații (RTR)[2] drept coordonator al serviciilor digitale (DSC) din țară.

RTR, în calitatea sa, este responsabilă de supravegherea și aplicarea cerințelor DSA în Austria. Aceasta include supravegherea respectării de către furnizorii de servicii digitale care operează în țară și coordonarea cu alte autorități naționale și europene pentru a asigura o aplicare consecventă a DSA în întreaga UE.

DSA urmărește să creeze un mediu online mai sigur și mai transparent prin impunerea de obligații serviciilor digitale care acționează ca intermediari între utilizatori și servicii, bunuri ori conținut. Aceste obligații cuprind măsuri de combatere a conținutului ilegal, de creștere a transparenței în publicitate și de protecție a drepturilor fundamentale ale utilizatorilor online.

---

[1] Titlu complet: Legea federală de promulgare a Legii privind coordonatorul serviciilor digitale și de modificare a Legii KommAustria, a Legii privind comerțul electronic, a Codului civil general, a Legii privind drepturile de autor, a Legii privind taxele judiciare, a Legii privind mass-media, a Codului de procedură penală din 1975, a Legii privind procuratura, a Legii federale privind cooperarea judiciară în materie penală cu statele membre ale Uniunii Europene, a Legii privind extrădarea și asistența judiciară reciprocă și a Legii privind telecomunicațiile 2021 (Legea de însoțire a DSA - DSA-BegG)

[2] Autoritatea austriacă de reglementare pentru radiodifuziune și telecomunicații (RTR) este o instituție de stat cu un mandat legal în ceea ce privește reglementarea, dezvoltarea și promovarea piețelor austriece pentru mass-media, telecomunicații și servicii poștale.
RTR a fost înființată la 1 aprilie 2001 prin Legea KommAustria (KOG). RTR este deținut în întregime de statul federal. RTR este alcătuită din două divizii specializate cu un total de 200 de angajați. Divizia Media și Divizia de telecomunicații și servicii poștale sunt conduse fiecare de un director general separat. Atribuțiile RTR sunt detaliate în Legea KommAustria (KOG) și în Legea telecomunicațiilor (TKG).

Pentru furnizorii de servicii digitale care își desfășoară activitatea în Austria, conformitatea cu DSA presupune aderarea la aceste obligații și cooperarea cu RTR pentru a asigura aplicarea eficientă a regulamentului. Având în vedere aplicabilitatea directă a DSA în toate statele membre ale UE, rolul RTR este esențial în interpretarea și aplicarea regulamentului în contextul austriac.

În Austria, cerința de verificare a identității în momentul înregistrării pe o platformă online depinde de natura platformei și de serviciile pe care le oferă.
Majoritatea platformelor, cum ar fi rețelele de socializare sau site-urile de comerț electronic, de obicei nu solicită utilizatorilor să prezinte un act de identitate oficial în timpul înregistrării. Platformele care oferă servicii în sectoare reglementate, cum ar fi serviciile bancare sau financiare, sunt obligate prin lege să verifice identitatea utilizatorilor lor. Acest lucru este în conformitate cu Legea privind combaterea spălării banilor (AMLA), care, începând din 2022, permite utilizarea diferitelor metode de verificare a identității la distanță, inclusiv verificarea online a documentelor și captura biometrică[3].
Platformele care oferă acces la conținut restricționat în funcție de vârstă pot implementa măsuri de verificare a vârstei pentru a controla accesul. Digital Services Act (DSA) al UE permite platformelor online să instituie astfel de măsuri pentru a proteja minorii de conținutul dăunător.

În Austria, protecția datelor cu caracter personal sensibile - cum ar fi informațiile privind originea rasială sau etnică, opiniile politice, convingerile religioase, apartenența sindicală, datele genetice, datele biometrice, informațiile privind sănătatea sau orientarea sexuală - este reglementată atât de Regulamentul general privind protecția datelor (GDPR), cât și de Legea austriacă privind protecția datelor Datenschutzgesetz sau DSG.
Legea austriacă privind protecția datelor (DSG) completează GDPR prin furnizarea de dispoziții naționale în domenii specifice, inclusiv reglementări privind prelucrarea datelor cu

[3] Procesul de colectare și utilizare a caracteristicilor biologice unice ale unei persoane - cum ar fi imaginile faciale sau amprentele digitale - în scopuri de identificare și autentificare. Această tehnologie este utilizată în diverse sectoare pentru a spori securitatea, a simplifica procesele și a respecta cerințele de reglementare.

caracter personal în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică sau în scopuri statistice.

Dispozițiile-cheie pentru protejarea datelor sensibile sunt:

- Consimțământul explicit, adică prelucrarea datelor cu caracter personal sensibile necesită, consimțământul explicit al persoanei, asigurându-se că aceasta este pe deplin informată și este de acord cu utilizarea specifică a datelor sale;
- Prelucrarea poate fi permisă în cazul în care este necesară pentru îndeplinirea obligațiilor în materie de angajare, securitate socială sau din motive de interes public substanțial, cu condiția existenței unor garanții adecvate;
- Datele sensibile pot fi prelucrate în scopuri medicale, cum ar fi diagnosticarea, furnizarea de îngrijire sau tratament sau gestionarea sistemelor de sănătate, în condiții stricte de confidențialitate.

Autoritatea austriacă pentru protecția datelor (Datenschutzbehörde) supraveghează respectarea legislației privind protecția datelor, oferind îndrumări și gestionând plângerile legate de activitățile de prelucrare a datelor.

Într-un caz notabil, Curtea Europeană de Justiție a hotărât că Meta (fostul Facebook) nu poate utiliza informații disponibile public cu privire la orientarea sexuală a unui utilizator pentru publicitate direcționată fără consimțământul explicit al persoanei. Această decizie evidențiază aplicarea strictă a legislației privind protecția datelor cu caracter personal sensibile în Austria.

Austria aplică măsuri solide de protecție a datelor cu caracter personal sensibile, aliniindu-se la reglementările UE și încorporând dispoziții naționale specifice pentru a aborda contexte unice și a asigura o protecție completă a datelor.

BELGIA

În Belgia, aplicarea Regulamentului (UE) 2022/2065 a trecut prin mai multe etape-cheie.

Belgia a făcut obiectul unei proceduri privind încălcarea dreptului comunitar/ infringement de către Comisia Europeană cu privire la DSA care impunea tuturor statelor membre ale UE să desemneze și să împuternicească coordonatori naționali pentru serviciile digitale până

la 17 februarie 2024 pentru a supraveghea punerea în aplicare a legii. Belgia nu a respectat acest termen, ceea ce a determinat Comisia să trimită o scrisoare de punere în întârziere la 25 iulie 2024, urmată de un aviz motivat la 16 decembrie 2024. Aceste măsuri au fost luate ca urmare a faptului că Belgia nu își desemnase și împuternicise CSD. Ca răspuns, Belgia a desemnat de atunci patru autorități competente pentru a pune în aplicare DSA în jurisdicția sa.

Punerea în aplicare a Regulamentului implică colaborarea între cele patru autorități competente desemnate, fiecare responsabilă pentru anumite regiuni și sectoare:

- Institutul belgian pentru servicii poștale și telecomunicații (BIPT/IBPT) supraveghează punerea în aplicare și asigurarea respectării DSA pe întreg teritoriul Belgiei în calitate de autoritate federală.
- Autoritatea flamandă de reglementare pentru mass-media (Vlaamse Regulator voor de Media, VRM) este responsabilă de supravegherea serviciilor de intermediere și de punerea în aplicare a DSA în cadrul Comunității Flamande.
- Consiliul Superior al Audiovizualului (Conseil Supérieur de l'Audiovisuel, CSA) își desfășoară activitatea în comunitatea francofonă și asigură conformitatea cu DSA pentru furnizorii de servicii relevante din jurisdicția sa.
- Consiliul Media (Medienrat) funcționează ca autoritate competentă pentru comunitatea germanofonă.

Aceste autorități asigură în mod colectiv aplicarea coerentă și eficientă a ASD pe întreg teritoriul Belgiei, ținând seama de diviziunile lingvistice și regionale unice ale țării.

La 31 ianuarie 2024, un proiect de lege (nr. 55K3799) a fost depus la Camera Reprezentanților din Belgia pentru a armoniza legislația națională cu cerințele DSA. Acest proiect de lege vizează alinierea legislației belgiene la obligațiile și standardele stabilite de Regulament.

Începând cu aprilie 2025, Belgia continuă să depună eforturi pentru a se conforma pe deplin DSA, abordând preocupările Comisiei Europene și integrând dispozițiile regulamentului în cadrul său juridic național.

În Belgia, necesitatea verificării identității în momentul înregistrării pe o platformă online variază în funcție de natura platformei și de serviciile pe care le oferă.

Platforme online generale (social media, comerț electronic, forumuri), de obicei, nu solicită utilizatorilor să prezinte un act de identitate oficial în timpul înregistrării. Platformele care oferă servicii reglementate (bănci, servicii financiare, telecomunicații, jocuri de noroc, servicii guvernamentale) sunt obligate prin lege să verifice identitatea utilizatorilor.

Legea din 18 septembrie 2017 privind prevenirea spălării banilor și a finanțării terorismului impune organizațiilor să pună în aplicare măsuri de precauție privind clientela, inclusiv verificarea identității, pentru a preveni spălarea banilor și finanțarea terorismului. De exemplu, autoritățile belgiene impun ca toate cartelele SIM să fie legate de numărul național de înregistrare al proprietarului, necesitând verificarea identității pentru serviciile de telecomunicații mobile.

Platformele care furnizează conținut sau servicii sensibile la vârstă trebuie să pună în aplicare mecanisme de verificare a vârstei pentru a preveni accesul minorilor. DSA pune accentul pe protecția minorilor online, încurajând platformele să adopte metode adecvate de verificare a vârstei. În Belgia, platformele de jocuri de noroc sunt obligate să verifice dacă utilizatorii au peste o anumită vârstă, fiind prevăzute sancțiuni în caz de nerespectare, inclusiv rambursări obligatorii.

Persoanele fizice și juridice care înregistrează un nume de domeniu ***.be*** sunt supuse unor proceduri de verificare a identității. DNS Belgia a implementat măsuri pentru a se asigura că solicitanții înregistrării furnizează o identificare valabilă pentru a preveni înregistrările frauduloase de domenii.

Belgia oferă soluții de identitate digitală precum *itsme*[4], permițând cetățenilor să își verifice identitatea online în siguranță. Lansat în 2017, itsme permite utilizatorilor să acceseze diverse servicii, inclusiv portaluri bancare și guvernamentale, prin conectarea identității lor la smartphone-ul lor.

[4] Itsme este o soluție de identitate și autentificare digitală din Belgia care permite utilizatorilor să își verifice identitatea în siguranță pentru serviciile online. Funcționează ca un act de identitate digital de încredere, permițând persoanelor să acceseze servicii guvernamentale, bancare, de asistență medicală și alte platforme fără a avea nevoie de parole tradiționale sau documente fizice. Autentificarea are loc prin intermediul aplicației Itsme de pe un smartphone, care necesită un cod PIN unic din 5 cifre sau autentificare biometrică.

În timp ce platformele online generale din Belgia nu solicită de obicei verificarea identității pentru înregistrare, sectoarele care implică servicii reglementate, conținut restricționat în funcție de vârstă și înregistrarea numelor de domeniu impun astfel de cerințe pentru a respecta obligațiile legale și a asigura siguranța utilizatorilor.

În Belgia, protecția datelor cu caracter personal sensibile este reglementată în principal de Regulamentul general privind protecția datelor (GDPR) și de Legea privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal („Legea privind protecția datelor"). Adoptată la 30 iulie 2018, această lege completează GDPR prin abordarea domeniilor în care legislația națională este autorizată să ofere specificații suplimentare. Acesta include dispoziții referitoare la prelucrarea datelor sensibile, la mecanismele de punere în aplicare și la înființarea Autorității belgiene pentru protecția datelor (DPA). APD este responsabilă de supravegherea respectării legislației privind protecția datelor, de oferirea de orientări și de soluționarea plângerilor legate de activitățile de prelucrare a datelor.

Dispozițiile cheie pentru protejarea datelor sensibile sunt:

- Consimțământul explicit, adică prelucrarea datelor cu caracter personal sensibile necesită consimțământul explicit al persoanei, asigurându-se că aceasta este pe deplin informată și este de acord cu utilizarea specifică a datelor sale;
- Prelucrarea poate fi permisă în cazul în care este necesară pentru îndeplinirea obligațiilor în materie de angajare, securitate socială sau din motive de interes public substanțial, cu condiția existenței unor garanții adecvate;
- Datele sensibile pot fi prelucrate în scopuri medicale, cum ar fi diagnosticarea, furnizarea de îngrijire sau tratament sau gestionarea sistemelor de sănătate, în condiții stricte de confidențialitate.

O specificitate națională este vârsta consimțământului: Belgia a stabilit vârsta la care minorii își pot da consimțământul valabil pentru prelucrarea datelor legate de serviciile societății informaționale la 13 ani, mai mică decât vârsta implicită de 16 ani prevăzută de GDPR.

Legea privind protecția datelor include dispoziții specifice care reglementează prelucrarea datelor legate de condamnări penale și infracțiuni, aliniindu-se la permisiunile GDPR pentru reglementarea națională în acest domeniu.

Nerespectarea reglementărilor privind protecția datelor poate duce la amenzi administrative semnificative. GDPR permite amenzi de până la 20 de milioane de euro sau 4% din cifra de afaceri anuală totală la nivel mondial a anului financiar precedent, luându-se în considerare valoarea cea mai mare. Legea belgiană privind protecția datelor introduce, de asemenea, sancțiuni penale pentru anumite încălcări, aplicabile atât operatorilor, cât și procesatorilor.

DANEMARCA

Danemarca a pus în aplicare în mod activ Regulamentul (UE) 2022/2065 pentru a asigura un mediu online mai sigur și responsabil.

În decembrie 2023, Parlamentul danez a adoptat Legea privind punerea în aplicare a DSA, care a intrat în vigoare la 17 februarie 2024. Aceasta aliniază legislația națională a Danemarcei la DSA, oferind un cadru pentru aplicarea acesteia în țară.

Danemarca a desemnat Autoritatea daneză pentru concurență și consumatori (DCCA) drept coordonatorul serviciilor digitale (DSC). DCCA este responsabilă de supravegherea aplicării și respectării DSA, asigurându-se că platformele online respectă dispozițiile regulamentului.

În data de 7 iunie 2024, DCCA a anunțat o investigație asupra platformei de vânzări online Temu cu privire la posibile încălcări ale DSA. Investigația se concentrează pe preocupări legate de vânzarea de produse ilegale și de sistemele inadecvate de prevenire a reapariției comercianților necinstiți suspendați anterior. Această acțiune subliniază angajamentul Danemarcei de a pune în aplicare DSA și de a asigura protecția consumatorilor online. Prin aceste măsuri, Danemarca își demonstrează dedicarea față de respectarea standardelor stabilite de DSA, promovând un mediu digital mai sigur și mai transparent pentru cetățenii săi.

În Danemarca, cerința de a prezenta un act de identitate oficial în momentul înregistrării pe o platformă online depinde de natura platformei și de serviciile acesteia.

De regulă, platformele online generale (social media, comerț electronic, forumuri) nu solicită utilizatorilor să prezinte o identificare oficială în timpul înregistrării. Utilizatorii își pot crea conturi folosind informații personale de bază, cum ar fi numele, adresa de e-mail și data nașterii.

Platformele care oferă servicii sensibile sau reglementate (bănci, servicii guvernamentale, asistență medicală) solicită utilizatorilor să își verifice identitatea utilizând MitID, sistemul național de identificare digitală din Danemarca. MitID este sistemul național utilizat pentru autentificarea sigură în cadrul serviciilor online, cum ar fi serviciile bancare, portalurile guvernamentale, asistența medicală și întreprinderile private. Acesta a înlocuit NemID în 2023 și asigură o securitate sporită și conformitatea cu reglementările UE.

Pentru a obține MitID, persoanele trebuie să aibă un număr de înregistrare civilă danez CPR și să își confirme identitatea, adesea folosind pașaport sau carte de identitate naționale valabile. MitID este esențial pentru accesul la servicii precum serviciile bancare online, raportarea fiscală și poșta digitală.

Platformele care oferă conținut adaptat vârstei pot implementa mecanisme de verificare a vârstei pentru a restricționa accesul minorilor. Deși nu toate aceste platforme necesită un act de identitate oficial, unele pot utiliza MitID în scopul verificării vârstei.

În Danemarca, protecția datelor cu caracter personal sensibile este reglementată de Regulamentul general privind protecția datelor (GDPR) și de legea națională daneză privind protecția datelor.

Legea privind dispozițiile suplimentare la Regulamentul privind protecția persoanelor fizice în legătură cu prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Legea daneză privind protecția datelor) a fost adoptată pentru a completa GDPR și include dispoziții referitoare la prelucrarea datelor sensibile, la mecanismele de aplicare și la înființarea Agenției daneze pentru protecția datelor (Datatilsynet). Agenția este responsabilă de supravegherea respectării legislației privind protecția datelor, oferă orientări și gestionează plângerile legate de prelucrarea datelor.

Dispozițiile cheie pentru protejarea datelor sensibile sunt:

- Consimțământul explicit, însemnând că prelucrarea datelor cu caracter personal sensibile necesită de obicei consimțământul explicit al persoanei, asigurându-se că aceasta este pe deplin informată și este de acord cu utilizarea specifică a datelor sale;
- Prelucrarea poate fi permisă în cazul în care este necesară pentru îndeplinirea obligațiilor în materie de ocupare a forței de muncă, securitate socială sau din motive de interes public substanțial, cu condiția existenței unor garanții adecvate;

- Datele sensibile pot fi prelucrate în scopuri medicale, cum ar fi diagnosticarea, furnizarea de îngrijire sau tratament sau gestionarea sistemelor de sănătate, în condiții stricte de confidențialitate.

Legea daneză privind protecția datelor include dispoziții specifice care reglementează prelucrarea datelor referitoare la condamnări penale și infracțiuni, aliniindu-se la permisiunile GDPR privind reglementarea națională în acest domeniu. Există dispoziții specifice în secțiunea 8 pentru prelucrarea acestei categorii de date. Astfel, autoritățile publice sunt autorizate să prelucreze date privind infracțiunile penale dacă acest lucru este strict necesar pentru îndeplinirea sarcinilor lor oficiale.

Organizațiile private pot prelucra astfel de date numai dacă au obținut consimțământul explicit al persoanei în cauză. Fără consimțământ explicit, entitățile private pot prelucra aceste date doar dacă este strict necesar pentru a urmări un interes legitim care prevalează în mod clar asupra intereselor persoanei vizate.

Aceste dispoziții garantează că prelucrarea datelor referitoare la condamnările penale și infracțiunile din Danemarca se realizează cu garanții stricte, echilibrând necesitatea prelucrării cu protecția drepturilor individuale.

Nerespectarea reglementărilor privind protecția datelor poate duce la amenzi administrative semnificative. GDPR prevede amenzi de până la 20 de milioane de euro sau 4% din cifra de afaceri anuală totală la nivel mondial a anului financiar precedent, luându-se în considerare valoarea cea mai mare. Legea daneză privind protecția datelor introduce, de asemenea, sancțiuni penale pentru anumite încălcări, aplicabile atât operatorilor, cât și procesatorilor.

FRANȚA

În Franța, aplicarea DSA implică atât respectarea de către platformele în cauză, cât și o organizare instituțională specifică pentru a pune în aplicare dispozițiile sale.

Legea nr. 2024-449 din 21 mai 2024 privind securizarea și reglementarea spațiului digital a desemnat ARCOM (Autorité de Régulation de la Communication Audiovisuelle et

Numérique) drept autoritate de reglementare sau coordonator al serviciilor digitale (DSC) pentru Franța. Aceasta :

- supraveghează platformele stabilite în Franța;
- primește rapoarte și plângeri privind nerespectarea DSA;
- poate impune sancțiuni (amenzi);
- cooperează cu Comisia Europeană (care își păstrează competența asupra platformelor foarte mari precum X, Facebook, TikTok etc.).

În funcție de mărimea și rolul lor, platformele online au obligații diferite. Astfel, toți intermediarii trebuie:

- să instituie mecanisme de raportare a conținutului ilegal,
- să justifice ștergerea conținutului sau a conturilor.

Platformele online (de exemplu, piețele, rețelele sociale) trebuie:

- să publice rapoarte de transparență,
- să pună în aplicare un sistem de gestionare a reclamațiilor.

Platforme online foarte mari (VLOP) au obligații mai stricte:

- audituri de risc,
- transparență privind algoritmii,
- limitarea dezinformării etc.

ARCOM poate impune amenzi de până la 6% din cifra de afaceri mondială anuală, măsuri corective (de exemplu, suspendarea serviciului). Deciziile pot fi atacate la Consiliul de Stat.
În Franța, înregistrarea pe o platformă online nu este, în general, condiționată de furnizarea unui act de identitate, dar există unele excepții în funcție de tipul platformei și de cerințele legale.
Așadar, cazul general este că nu este necesar niciun ID pentru majoritatea platformelor precum: rețele sociale (Instagram, TikTok, X, etc.), comerț electronic (Amazon, Vinted, etc.), platforme de streaming sau media (YouTube, Netflix, etc.). Înregistrarea se face cu o adresă de e-mail, un nume de utilizator și o parolă - niciun act de identitate nu este obligatoriu prin lege în Franța.

Poate fi necesar un act de identitate în cazul platformelor cu tranzacții financiare, piețele online (de exemplu, Vinted, Leboncoin, Etsy). Acestea pot solicita un act de identitate pentru a verifica utilizatorii care devin vânzători, pentru a respecta reglementările privind combaterea spălării banilor (AML) și reglementările fiscale. Acest lucru se datorează reglementărilor franceze și UE (de exemplu, DAC7, AMLD).

Platformele care oferă conținut pentru adulți, jocuri de noroc sau anumite jocuri video ar putea solicita verificarea vârstei, care ar putea implica cartea de identitate sau alte metode. Franța face presiuni pentru o verificare mai strictă a vârstei - de exemplu: ARCOM poate solicita site-urilor pentru adulți să verifice vârsta utilizatorilor cu ajutorul unor instrumente eficiente, nu doar prin autodeclarare.

Serviciile precum furnizorii de semnături digitale, serviciile de sănătate sau platformele guvernamentale (de exemplu, FranceConnect) necesită un act de identitate pentru acces.

Datele cu caracter personal sensibile sunt protejate în Franța în temeiul unui cadru juridic solid care combină Regulamentul general al UE privind protecția datelor (GDPR) cu legislația franceză.

Regulamentul general al UE privind protecția datelor este aplicabil din 25 mai 2018 și stabilește reguli stricte, inclusiv în Franța, pentru gestionarea tuturor datelor cu caracter personal, cu garanții speciale pentru datele sensibile.

Legea franceză privind protecția datelor Loi Informatique et Libertés (Legea privind protecția datelor din 1978), modificată pentru a se alinia la GDPR, asigură aplicarea la nivel național și completează GDPR cu norme locale, (de exemplu, pentru minori, organisme publice, date privind sănătatea.

Principalele măsuri de protecție în Franța sunt:

- Temeiul juridic strict înseamnă că datele sensibile pot fi prelucrate numai dacă persoana vizată și-a dat consimțământul explicit, este necesar pentru dreptul muncii, interese vitale, pretenții legale, interes public în domeniul sănătății publice etc. Ca exemplu: un spital poate prelucra date de sănătate pentru îngrijirea pacienților; un site web nu poate colecta date etnice fără consimțământ explicit și un motiv legal.

- Minimizarea datelor și limitarea scopului; acesta înseamnă că pot fi colectate numai datele care sunt strict necesare pentru un scop specificat. Se interzice reutilizarea datelor în alte scopuri fără consimțământul persoanei.
- Securitatea și confidențialitatea impun operatorilor de date să pună în aplicare măsuri tehnice și organizaționale (criptare, control al accesului, pseudonimizare), să asigure confidențialitatea și formarea personalului.
- Transparența și drepturile persoanelor fizice înseamnă că în Franța, persoanele fizice au dreptul de acces, rectificare, ștergere, restricționare sau opoziție la prelucrarea datelor lor, dreptul de a depune o plângere la autoritatea franceză pentru protecția datelor, CNIL (Commission nationale de l'informatique et des libertés), dreptul la portabilitatea datelor.

CNIL este autoritatea independentă de reglementare care pune în aplicare GDPR și Legea franceză privind protecția datelor. Aceasta poate să efectueze audituri și investigații, emite avertismente sau sancțiuni, să impună amenzi (până la 20 de milioane de euro sau 4% din cifra de afaceri globală).
De exemplu: CNIL a amendat Google și Facebook pentru încălcarea politicii privind cookie-urile și TikTok pentru probleme de transparență a datelor.

GERMANIA

Pentru a facilita punerea efectiv în aplicare a DSA în cadrul juridic al Germaniei, guvernul german a adoptat Legea serviciilor digitale (Digitale-Dienste-Gesetz sau DDG). DDG a fost promulgată la 13 mai 2024 și a intrat în vigoare la 14 mai 2024.
DDG nu impune verificarea identității pentru utilizatori. Cu toate acestea, solicită platformelor să ofere o trasabilitate clară a comercianților - astfel încât vânzătorii și furnizorii de servicii de pe piețele online trebuie să își verifice identitatea, inclusiv, eventual, printr-un act de identitate.

Utilizarea anonimă este permisă într-o anumită măsură. Germania are o tradiție puternică în ceea ce privește protecția datelor și anonimatul online (înrădăcinată în Telemediengesetz[5] și continuată în DDG). Astfel, utilizatorii pot participa adesea la forumuri, bloguri sau platforme fără a-și dezvălui identitatea reală.

Cu toate acestea, platformele trebuie să asigure mecanisme de eliminare a conținutului ilegal și de identificare a utilizatorilor în cazul unor anchete judiciare.

Legea serviciilor digitale DDG desemnează Agenția Federală pentru Rețele (Bundesnetzagentur) drept coordonator al serviciilor digitale din Germania (DSC), responsabil cu supravegherea și aplicarea dispozițiilor DSA la nivel național[6]. Aceasta include supravegherea conformității de către furnizorii intermediari de servicii și coordonarea cu alte autorități relevante.

În plus, DDG atribuie responsabilități specifice altor autorități naționale:

- Oficiul Federal de Poliție Criminală (Bundeskriminalamt sau BKA) servește drept organism central pentru primirea și prelucrarea notificărilor din partea furnizorilor de servicii de găzduire cu privire la conținutul care poate constitui o amenințare la adresa vieții sau a siguranței, în conformitate cu articolul 18 din DSA.
- Autoritățile mass-media de stat și Agenția federală pentru protecția copiilor și tinerilor în mass-media (Bundeszentrale für Kinder und Jugendmedienschutz) sunt însărcinate cu chestiuni legate de protecția minorilor în mass-media.
- Comisarul federal pentru protecția datelor și libertatea de informare (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit) se ocupă de chestiuni privind publicitatea online și protecția datelor.

DDG introduce, de asemenea, sancțiuni pentru nerespectarea DSA, amenzile putând ajunge, în anumite cazuri, până la 6% din cifra de afaceri anuală mondială a unei societăți.

[5] Legea Telemedia (Telemediengesetz TMG) a expirat la 14 mai 2024 și a fost înlocuită de Legea serviciilor digitale (DDG).

[6] Bundesnetzagentur (Agenția Federală de Rețele) este o autoritate de reglementare cheie în Germania, cu responsabilități extinse în mai multe sectoare de rețea: electricitate, gaze, telecomunicații, poștă și căi ferate. Competențele sale includ supravegherea, reglementarea pieței și protecția consumatorilor. În domeniul telecomunicațiilor, reglementează rețelele și serviciile de telecomunicații, supraveghează alocarea frecvențelor, planurile de numerotare și accesul pe piață, protejează drepturile consumatorilor (de exemplu, transparența vitezei în bandă largă, executarea contractelor), promovează concurența și dezvoltarea infrastructurii.

În Germania, înregistrarea pe o platformă online nu este, în general, condiționată de prezentarea unui act de identitate - însă există excepții importante în funcție de tipul platformei, de serviciile oferite și de legile și reglementările relevante.
Pentru majoritatea platformelor social media, forumurilor sau site-urilor de cumpărături, utilizatorii se pot înregistra folosind doar o adresă de e-mail sau un număr de telefon. Verificarea identității nu este obligatorie în temeiul legislației germane în cazurile generale.
Din iulie 2017, ca urmare a Legii antiterorism, verificarea identității este obligatorie pentru achiziționarea de cartele SIM preplătite. Este necesar un act de identitate valabil emis de guvern (în persoană sau prin verificare video).
Platformele care oferă servicii financiare trebuie să respecte reglementările privind combaterea spălării banilor (AML). Verificările de cunoaștere a clientelei (KYC[7]) necesită verificarea completă a identității înainte de utilizare.
Platformele cu conținut restricționat în funcție de vârstă (de exemplu, platforme pentru adulți, jocuri de noroc) sunt obligate prin lege să verifice vârsta unui utilizator pentru a restricționa accesul minorilor. Aceasta implică adesea verificarea actului de identitate sau verificarea oficială a vârstei.
Platforme de închiriere (de exemplu, gazdele Airbnb, unele servicii de ride-sharing) pot solicita un act de identitate pentru a verifica identitatea utilizatorului, în special pentru gazde sau furnizori, nu întotdeauna pentru oaspeți/clienți.

În Germania, datele personale sensibile sunt protejate în temeiul unor legi stricte privind confidențialitatea, în principal prin GDPR. Acesta este direct aplicabil în Germania și reprezintă cadrul juridic de bază pentru protecția datelor. Tipurile de date sensibile sunt supuse unor norme de prelucrare mai stricte. Prelucrarea lor este interzisă, cu excepția cazului în care:

- persoana fizică și-a dat consimțământul explicit;
- este necesară pentru ocuparea forței de muncă, protecție socială sau îngrijire medicală;
- pentru motive de interes public;

[7] Engl.: know your client

- pentru acțiuni în justiție sau funcții judiciare;
- datele sunt deja făcute publice de către persoana respectivă.

BDSG (Bundesdatenschutzgesetz - Legea federală privind protecția datelor) completează GDPR în Germania. Specifică modul în care organismele publice și anumite sectoare (de exemplu, ocuparea forței de muncă, sănătate, cercetare) trebuie să gestioneze datele sensibile. Legea numește Comisarul federal pentru protecția datelor și libertatea de informare (BfDI[8]) ca autoritate de supraveghere cheie. Comisarul federal pentru protecția datelor și libertatea de informare (BfDI) este autoritatea independentă din Germania responsabilă cu supravegherea protecției datelor și a libertății de informare la nivel federal. Acest rol include supravegherea organismelor publice federale și a anumitor sectoare, precum telecomunicațiile și serviciile poștale, pentru respectarea legislației privind protecția datelor.

Măsuri specifice pe domenii de activitate:

- Sectorul ocupării forței de muncă: angajatorii pot prelucra date sensibile numai atunci când este absolut necesar (de exemplu, pentru sănătatea la locul de muncă sau respectarea legislației muncii);
- Sectorul sănătății: norme speciale în temeiul SGB V (Codul Social) și al legilor privind confidențialitatea medicală;
- Cercetarea este permisă în condiții de garanții stricte și, de obicei, de pseudonimizare/anonimizare.

Măsurile de securitate și de conformitate includ:

- Evaluări ale impactului asupra protecției datelor (DPIA) sunt obligatorii pentru prelucrarea cu risc ridicat (de exemplu, date privind sănătatea pe scară largă);
- Pseudonimizarea/ anonimizarea sunt încurajate sau obligatorii pentru reducerea riscurilor;
- Criptarea și controlul accesului reprezintă garanții tehnice standard;
- În caz de descoperire a unei încălcări, trebuie notificată autoritatea în termen de 72 de ore.

[8] Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit", care se traduce prin Comisarul federal pentru protecția datelor și libertatea de informare în Germania

Consimțământul pentru procesarea datelor trebuie să fie:

- Explicit pentru datele sensibile (casetele de selectare nu trebuie bifate în prealabil);
- Informat - utilizatorii trebuie să știe ce se colectează și de ce;
- Acordat în mod liber - nu este o condiție pentru accesarea unor servicii care nu au legătură cu acesta.

BfDI supraveghează instituțiile federale și serviciile de telecomunicații/ postale. Autoritățile pentru protecția datelor la nivel de land (Landesdatenschutzbehörden) supraveghează companiile private și instituțiile de stat și pot impune amenzi mari (până la 20 de milioane EUR sau 4% din cifra de afaceri globală în temeiul GDPR).

Cadrul de supraveghere pentru protecția datelor și libertatea de informare în Germania este structurat la nivel federal. Pe lângă supravegherea de către autoritățile de stat și locale, sectorul non-public este supravegheat, în general, de către autoritățile de land responsabile pentru protecția datelor. În cazul în care există o lege privind libertatea de informare sau transparența în statul federal respectiv, comisarii de stat/land acționează, de asemenea, ca autorități independente de supraveghere. Acest lucru nu se aplică în Bavaria, Saxonia Inferioară și Saxonia, deoarece aceste state nu au adoptat o lege corespunzătoare.

BfDI[9] investighează adesea încălcări ale securității datelor și ale vieții private, în special în cazul agențiilor guvernamentale sau al marilor corporații. Câteva exemple includ:

În 2019, BfDI a luat măsuri împotriva unui furnizor de telecomunicații despre care s-a constatat că a gestionat în mod necorespunzător datele personale a milioane de clienți, încălcând normele GDPR. Problema a fost legată de practicile de păstrare a datelor, în care datele privind apelurile personale și informațiile sensibile au fost păstrate mai mult decât era permis. BfDI a impus sancțiuni, a solicitat acțiuni corective și a subliniat necesitatea unor măsuri adecvate de securitate a datelor.

[9] De asemenea, BfDI se ocupă de plângerile privind accesul la informațiile deținute de guvern, asigurându-se că publicul poate avea acces la documente, cu excepția cazului în care se aplică o excepție legală valabilă. Transparență în contractele guvernamentale. Cererea unui cetățean de a obține informații privind contractele guvernamentale cu companii private a fost respinsă pe motiv de secret de afaceri. BfDI a decis în favoarea cetățeanului, ordonând guvernului să facă publice o parte dintre documente, subliniind dreptul publicului la transparență în ceea ce privește cheltuielile publice.

În sectorul sănătății, BfDI a investigat cazuri în care datele privind sănătatea au fost partajate fără consimțământ de către organizațiile de sănătate publică, ceea ce a condus la amenzi semnificative și la modificări ale protocoalelor interne de gestionare a datelor.
BfDI a emis, de asemenea, declarații și avize cu privire la probleme emergente legate de confidențialitatea digitală, instrumentele de supraveghere și transferurile internaționale de date.
În 2020, BfDI a criticat acordul Privacy Shield UE-SUA după ce Curtea de Justiție a Uniunii Europene (CJUE) l-a declarat invalid. Acest lucru s-a întâmplat în lumina preocupărilor legate de programele de supraveghere ale SUA care au încălcat standardele europene de confidențialitate. Declarația BfDI a subliniat necesitatea unor garanții mai bune pentru datele cu caracter personal transferate transfrontalier, în special către SUA.
În 2022, BfDI a emis un aviz public împotriva utilizării tehnologiei de recunoaștere facială în locuri publice precum centre comerciale sau gări, fără motive juridice clare. Acesta și-a exprimat îngrijorarea cu privire la încălcarea dreptului la viață privată și a solicitat reglementări stricte înainte ca astfel de tehnologii să poată fi utilizate în spațiile publice.
În 2021, BfDI a amendat o mare platformă de social media pentru încălcarea drepturilor persoanelor vizate de GDPR, cum ar fi faptul că nu a permis utilizatorilor să aibă acces ușor la datele lor și nu a oferit o modalitate de a-și exercita dreptul la ștergere. Li s-a ordonat să își îmbunătățească practicile de conformitate și să ofere politici mai clare de prelucrare a datelor.
BfDI intervine și atunci când agențiile guvernamentale nu reușesc să protejeze datele. De exemplu, dacă un organism guvernamental nu dispune de practici adecvate de securitate cibernetică, BfDI poate emite avertismente și impune măsuri corective.

IRLANDA

Pentru a facilita implementarea și aplicarea efectivă a Regulamentului (UE) 2022/2065 în Irlanda, această țară a adoptat Legea serviciilor digitale 2024, care a intrat în vigoare la 17 februarie 2024.

Unul dintre aspectele cheie ale aplicării DSA în Irlanda este desemnarea Coimisiún na Meán în calitate de coordonator al serviciilor digitale (DSC). Coimisiún na Meán, înființată la 15 martie 2023, îndeplinește funcția de autoritate de reglementare a mass-media și a radiodifuziunii din Irlanda.

Deși DSA este direct aplicabilă, Legea serviciilor digitale 2024 din Irlanda integrează dispozițiile acesteia în legislația națională, asigurând un cadru juridic coerent pentru serviciile digitale. Această integrare implică modificări ale legislației existente, cum ar fi Legea radiodifuziunii din 2009, pentru a răspunde cerințelor DSA.

Coimisiún na Meán are sarcina de a monitoriza conformitatea în rândul furnizorilor de servicii digitale care operează în Irlanda. Aceasta are autoritatea de a investiga eventualele încălcări și de a impune sancțiuni pentru a asigura respectarea DSA.

De exemplu, în noiembrie 2024, Coimisiún na Meán a ordonat unor platforme precum X (fostul Twitter), TikTok și Instagram să pună în aplicare măsuri de prevenire a difuzării de conținut terorist în aplicarea standardelor de siguranță online.

În Irlanda, cerința de a furniza un act de identitate (ID) la înregistrarea pe o platformă online variază în funcție de natura platformei și de serviciile pe care le oferă.

Pentru accesul la diverse servicii publice online, Irlanda utilizează MyGovID, un sistem securizat de verificare a identității. Un cont MyGovID de bază necesită doar o adresă de e-mail. Cu toate acestea, pentru a accesa servicii de valoare mai mare, este necesar un cont MyGovID verificat. Verificarea pentru un cont MyGovID implică de obicei prezentarea unor documente oficiale de identificare, cum ar fi un card de servicii publice (PSC) sau un pașaport, pentru autentificarea identității.

În general, platformele din sectorul privat, precum rețelele de social media sau comercianții cu amănuntul online nu impun verificarea identității la înregistrare. Cu toate acestea, anumite activități (de exemplu, tranzacții de mare valoare, conținut restricționat în funcție de vârstă) pot determina aceste platforme să solicite verificarea identității pentru a respecta obligațiile legale sau politicile interne.

Băncile online și instituțiile financiare sunt obligate prin lege să verifice identitatea clienților lor în conformitate cu reglementările privind combaterea spălării banilor (AML). Acest proces, cunoscut sub denumirea de „cunoașteți-vă clientul” (KYC), necesită, de obicei,

prezentarea unor documente oficiale de identificare în timpul procesului de creare a contului.

Pe scurt, în timp ce verificarea identității este o cerință standard pentru accesarea multor servicii guvernamentale online în Irlanda, necesitatea acesteia în sectorul privat depinde de platforma specifică și de natura serviciilor furnizate.

În Irlanda, protecția datelor cu caracter personal sensibile - cunoscute și ca date din categorii speciale în conformitate cu GDPR - este luată foarte în serios și este reglementată de: Regulamentul general al UE privind protecția datelor (GDPR), direct aplicabil în întreaga UE, Legea națională irlandeză privind protecția datelor din 2018, care completează și pune în aplicare GDPR precum și supravegherea de către autoritatea națională pentru protecția datelor din Irlanda, Data Protection Commission (DPC). Datele cu caracter personal sensibile beneficiază de un nivel ridicat de protecție prin măsuri juridice cuprinzătoare, standarde stricte de prelucrare, cerințe solide de securitate și supravegherea activă de către Comisia pentru protecția datelor. Aceste garanții asigură respectarea dreptului la viață privată al persoanelor și faptul că orice prelucrare a datelor sensibile este efectuată în mod sigur și legal.

Principiile cheie în privința protecției datelor sensibile sunt:

- Consimțământul explicit care înseamnă că prelucrarea datelor sensibile necesită de obicei consimțământul clar, informat și explicit al persoanei, cu excepția cazului în care se aplică un alt temei juridic (cum ar fi dreptul muncii, interesele vitale sau sănătatea publică);
- Limitarea scopului și minimizarea datelor, ceea ce presupune că operatorii de date trebuie să colecteze și să prelucreze date numai în scopuri specificate, explicite și legitime și să se asigure că datele colectate sunt limitate la ceea ce este necesar pentru acele scopuri;
- Transparența, adică organizațiile trebuie să furnizeze informații clare cu privire la datele prelucrate, la modul în care acestea sunt utilizate și la persoanele cu care pot fi partajate. Această transparență împuternicește persoanele să înțeleagă și să controleze datele lor cu caracter personal.

Există și o serie de măsuri de securitate, care cuprind garanții tehnice, măsuri organizaționale și evaluări de impact. Garanțiile tehnice constau în măsuri de securitate de

ultimă generație, cum ar fi criptarea, controlul accesului și evaluări periodice ale securității pentru a proteja datele împotriva accesului neautorizat sau a încălcărilor. Măsurile organizaționale includ politici, formarea personalului și procese pentru a asigura conformitatea cu legislația privind protecția datelor și pentru a aborda cu promptitudine orice vulnerabilități potențiale. Evaluări ale impactului asupra protecției datelor (DPIA) sunt obligatorii pentru activitățile de prelucrare care pot prezenta un risc ridicat pentru drepturile și libertățile persoanelor. Acest lucru ajută organizațiile să identifice și să reducă riscurile asociate cu prelucrarea datelor sensibile.

Drepturile persoanelor vizate se referă la faptul că persoanele fizice au dreptul de a-și accesa datele cu caracter personal și de a solicita corecții în cazul în care se constată inexactități; ștergerea și restricționarea, cunoscut ca „dreptul de a fi uitat”, persoanele fizice pot solicita ștergerea sau restricționarea datelor lor în anumite condiții. Portabilitatea datelor înseamnă că persoanele fizice au dreptul de a primi datele lor într-un format structurat, utilizat în mod obișnuit și de a le transfera unui alt operator. Persoanele fizice se pot opune prelucrării datelor, în special în cazurile care implică decizii automatizate cu efecte semnificative asupra lor.

Comisia pentru protecția datelor (DPC) din Irlanda este responsabilă cu monitorizarea și asigurarea respectării legislației privind protecția datelor. Aceasta poate investiga plângerile, efectua audituri și impune amenzi semnificative (de până la 4% din cifra de afaceri anuală globală sau 20 de milioane EUR, luându-se în considerare valoarea cea mai mare) pentru nerespectarea legislației.

Atât entitățile publice, cât și cele private pot fi supuse unor audituri și inspecții pentru a se asigura că respectă cerințele stricte privind gestionarea datelor cu caracter personal sensibile.

Un exemplu de măsură de protecție a datelor este amenda de 225 de milioane EUR pentru WhatsApp Irlanda în 2021. Comisia pentru protecția datelor (DPC) a constatat că WhatsApp Irlanda nu a oferit suficientă transparență utilizatorilor și neutilizatorilor cu privire la modul în care datele lor au fost prelucrate și partajate cu Facebook (Meta). Aceasta a fost o încălcare a obligațiilor de transparență ale GDPR (articolele 13 și 14). În consecință, WhatsApp a fost amendată cu 225 de milioane EUR, una dintre cele mai mari amenzi GDPR din UE la

momentul respectiv. Aceasta a fost obligată să își actualizeze politica și procesele de confidențialitate.

Un alt caz au fost schemele de fidelizare și supraveghere a comerțului cu amănuntul: mai multe lanțuri irlandeze de magazine au fost examinate de DPC pentru utilizarea cardurilor de fidelitate și a sistemelor CCTV. În unele cazuri camerele de supraveghere au capturat mai multe date decât era necesar (de exemplu, înregistrarea trotuarelor publice), iar programele de fidelizare nu explicau în mod clar modul în care datele clienților ar fi utilizate pentru crearea de profiluri sau marketing. Utilizarea datelor biometrice în școli este un alt exemplu de utilizare a datelor sensibile: o școală secundară din Irlanda a instalat sisteme de recunoaștere facială pentru a urmări prezența elevilor fără consimțământul sau necesitatea corespunzătoare. DPC a intervenit în 2021, declarând că sistemul era disproporționat și ilegal în conformitate cu GDPR, în special deoarece implica date biometrice, care sunt extrem de sensibile.

LUXEMBURG

La 2 aprilie 2025, Parlamentul luxemburghez a adoptat legislația care desemnează Autoritatea luxemburgheză pentru concurență (Autorité de la Concurrence) ca DSC național. Această autoritate are sarcina de a supraveghea și de a impune respectarea DSA de către furnizorii de servicii digitale cu sediul în Luxemburg.

Legislația, cunoscută sub numele de proiectul de lege 8309[10], integrează DSA în legislația națională a Luxemburgului. Aceasta modifică legile existente, inclusiv Legea modificată din 14 august 2000 privind comerțul electronic și Legea modificată din 04 aprilie 2022 privind concurența.

În calitate de DSC, Autorité de la Concurrence este responsabilă pentru monitorizarea conformității, mai precis asigurarea că platformele online stabilite în Luxemburg respectă dispozițiile DSA.

[10] La data de 2 aprilie 2025, proiectul de lege 8309 a fost adoptat de Parlamentul luxemburghez și urmează să fie publicat în jurnalul oficial pentru a intra în vigoare.

DSC are rol și de autoritate de investigare și impune sancțiuni, inclusiv amenzi de până la 6% din cifra de afaceri anuală globală a platformei pentru încălcări ale DSA. Pentru protecția consumatorilor acționează ca punct de contact pentru consumatori în vederea raportării conținutului ilegal și a aplicării interdicțiilor privind publicitatea adresată minorilor; pentru promovarea transparenței, prin algoritmii de recomandare și în sistemele de publicitate de pe platformele digitale.

Având în vedere natura multifațetată a serviciilor digitale, Autoritatea pentru Concurență din Luxemburg colaborează cu alte organisme naționale, printre care:

- CNPD (Comisia Națională pentru Protecția Datelor) pentru abordarea problemelor legate de protecția datelor și a vieții private;
- ALIA (Autoritatea audiovizuală independentă din Luxemburg) pentru supravegherea reglementărilor privind conținutul audiovizual;
- ILNAS (Institutul luxemburghez pentru standardizare, acreditare, siguranță și calitate a produselor și serviciilor) legat de standardele de siguranță ale produselor;
- agenții de aplicare a legii pentru coordonarea aspectelor care necesită aplicarea legii.

Platformele digitale care operează în Luxemburg trebuie să respecte obligațiile DSA, care includ moderarea conținutului, protecția drepturilor utilizatorilor, asigurarea respectării drepturilor lor online, transparența publicității adică furnizarea de informații clare cu privire la practicile de publicitate și asigurarea responsabilității în ceea ce privește plasarea reclamelor.

Neconformitatea poate duce la sancțiuni semnificative, subliniind importanța ca platformele să își alinieze operațiunile la cerințele DSA.

În Luxemburg, datele cu caracter personal sensibile - cunoscute și sub denumirea de categorii speciale de date cu caracter personal - sunt puternic protejate atât de legislația UE, cât și de legislația națională. Cele două cadre juridice principale sunt Regulamentul GDPR și Legea din 1 august 2018. Această lege pune în aplicare și completează GDPR la nivel național. Mai precis, stabilește competențele Comisiei Naționale pentru Protecția Datelor (Commission nationale pour la protection des données CNPD), autoritatea națională pentru protecția datelor, include norme naționale privind: prelucrarea datelor pentru anchete

penale, prelucrarea specifică în domeniul ocupării forței de muncă și în sectorul public, cerințele privind notificarea încălcării securității datelor.

În 2022, CNPD a amendat o bancă cu 10 000 EUR pentru încălcarea dispozițiilor GDPR referitoare la minimizarea și transparența datelor pentru că banca instalase camere de supraveghere fără a informa în mod corespunzător persoanele vizate și a filmat în mod continuu unele persoane.

În iulie 2021, CNPD a impus Amazon o amendă record de 746 de milioane EUR. S-a constatat că Amazon Europe Core S.à.r.l. prelucrase date cu caracter personal cu încălcarea principiilor GDPR. Amazon a contestat decizia; cu toate acestea, în martie 2025, instanța administrativă din Luxemburg a respins apelul, menținând amenda stabilită de CNPD.

POLONIA

Regulamentul (UE) 2022/2065 a devenit direct aplicabil în Polonia, la 17 februarie 2024, la fel ca în toate statele membre ale Uniunii Europene.

Pentru a pune în aplicare DSA, fiecare stat membru al UE trebuie să desemneze un coordonator al serviciilor digitale (DSC) - o autoritate națională responsabilă de supravegherea respectării regulamentului. Cu toate acestea, Polonia a întâmpinat dificultăți. Drept răspuns, Comisia Europeană a inițiat proceduri privind încălcarea dreptului comunitar, trimițând Poloniei, la 16 decembrie 2024, un aviz motivat prin care îi solicita să se conformeze.

În prezent, Polonia este singura țară din UE care nu are un coordonator al serviciilor digitale[11] pentru a pune în aplicare dispozițiile Regulamentului privind serviciile digitale, care este esențial pentru industria internetului. Au avut loc deja 12 reuniuni ale unor astfel de reprezentanți din alte țări, însă Polonia nu participa, întrucât nu are un coordonator desemnat.

[11] https://www.euractiv.com/section/tech/news/poland-fails-to-appoint-digital-democracy-watchdog-ahead-of-election/

Ministerul polonez al digitalizării a lucrat la elaborarea legislației pentru punerea în aplicare a DSA pe plan intern. Legea propusă vizează înființarea DSC. Discuțiile au luat în considerare numirea președintelui Oficiului pentru comunicații electronice (UKE) în calitate de DSC, cu implicarea potențială a Oficiului pentru concurență și protecția consumatorilor (UOKiK).

Consiliul Național de Radiodifuziune din Polonia exprimă în mod oficial opinii[12] referitoare la proiectul de lege menționat mai sus, concluzionând că ”aplicarea (...) prezintă un risc ridicat de a fi utilizată pentru eliminarea discursurilor critice de pe internet, încălcând dreptul fundamental la libertatea de exprimare.”

Între timp, întreprinderile poloneze care oferă servicii digitale sunt sfătuite să își alinieze în mod proactiv operațiunile la cerințele DSA. Aceasta include punerea în aplicare a mecanismelor de moderare a conținutului, asigurarea transparenței în publicitate și

[12] Politizarea punerii în aplicare a DSA în Polonia și riscul rezultat al cenzurării conținutului internetului
DSA, care este un act de drept al UE, nu este o reglementare a conținutului online într-un anumit stat membru, ci o reglementare a procedurilor de diligență de către furnizorii de servicii intermediare în sensul DSA.
Îndeplinirea acestui obiectiv nu este îndeplinită de ultimul proiect de lege de punere în aplicare a DSA în ordinea juridică poloneză, care a introdus modificări semnificative în comparație cu versiunea anterioară a acestui proiect. În plus, aceste modificări au fost introduse după încheierea consultărilor publice (de două ori), ceea ce privează utilizatorii de internet și instituțiile publice de posibilitatea de a se referi în mod colectiv la acestea și de a afla reacția redactorilor.
Modificările propuse includ:
- o extindere semnificativă a competențelor președintelui UKE, care va putea emite ordine pentru a lua măsuri împotriva conținutului ilegal din serviciile furnizate de furnizorii de servicii intermediare nu numai împotriva conținutului care încalcă drepturile de proprietate intelectuală (ca în versiunea anterioară a proiectului), ci și împotriva conținutului care încalcă drepturile personale și a cărui difuzare îndeplinește condițiile unui act interzis. În versiunea anterioară a proiectului, aceste competențe erau atribuite unei instanțe și nu președintelui UKE;
- o slăbire semnificativă a garanțiilor procedurale care ar trebui să garanteze egalitatea părților în fața legii și imparțialitatea deplină, independența și competența adecvată a organismului decizional, în timp ce acest proiect de lege de punere în aplicare a DSA prevede următoarele elemente care slăbesc aceste garanții:
    1. lipsa participării utilizatorilor la procedurile UKE;
    2. lipsa de experiență a UKE în soluționarea cazurilor individuale în ceea ce privește echilibrarea valorilor protejate, cum ar fi libertatea de exprimare față de protecția împotriva discriminării, protecția drepturilor personale;
    3. garanții insuficient de solide ale independenței UKE față de guvern în contextul elaborării unor competențe extinse pentru acest organism în domenii sensibile privind restrângerea libertății de exprimare;
    4. rigoarea punerii în aplicare imediate a deciziei președintelui UKE;
    5. posibilitatea de a ataca decizia președintelui UKE nu la o instanță de drept comun, ci la o instanță administrativă, care nu are competență și experiență în soluționarea litigiilor privind libertatea de exprimare, ale cărei decizii se referă la legalitatea aspectelor procedurale, nu la cele de fond.

https://www.gov.pl/web/krrit-en/risks-and-threats-associated-with-the-polish-governments-conduct-to-date-in-relation-to-the-implementation-of-the-digital-services-act-dsa-to-the-polish-legal-system2

stabilirea de proceduri pentru abordarea conținutului ilegal. Nerespectarea legislației poate duce la sancțiuni semnificative, inclusiv amenzi de până la 6 % din cifra de afaceri anuală la nivel mondial.

Pe scurt, deși DSA este direct aplicabilă în Polonia, aplicarea deplină a acesteia depinde de înființarea oficială și împuternicirea DSC naționale. Se depun în prezent eforturi pentru a remedia aceste lacune și pentru a asigura respectarea deplină a regulamentului.

În Polonia, cerința de a furniza un act de identitate la înregistrarea pe o platformă online variază în funcție de tipul de serviciu și de politicile specifice ale platformei. Accesarea serviciilor guvernamentale online necesită, de obicei, verificarea identității prin intermediul unor sisteme precum Trusted Profile sau mojeID.

Trusted Profile (Profil Zaufany) permite utilizatorilor să își autentifice identitatea pentru serviciile de e-guvernare. Crearea acestui profil necesită un număr PESEL (numărul național de identificare polonez) și poate fi autentificat prin intermediul serviciilor bancare electronice sau personal la punctele desemnate.

MojeID permite utilizatorilor să își verifice identitatea online prin intermediul serviciilor electronice ale băncii lor, facilitând accesul securizat la serviciile din sectorul public și privat. Băncile online și instituțiile financiare sunt obligate prin lege să efectueze proceduri de cunoaștere a clientelei (KYC). Acestea implică verificarea identității clientului cu ajutorul documentelor oficiale pentru a respecta reglementările privind combaterea spălării banilor.

În general, platformele precum comercianții cu amănuntul online și rețelele de social media nu impun verificarea identității la înregistrare. Cu toate acestea, anumite activități, cum ar fi tranzacțiile de mare valoare sau accesarea de conținut restricționat în funcție de vârstă, pot determina aceste platforme să solicite verificarea identității pentru a respecta obligațiile legale sau politicile interne.

În Polonia, protecția datelor cu caracter personal sensibile - denumite și categorii speciale de date cu caracter personal - este reglementată în principal de Regulamentul GDPR și Legea privind protecția datelor din 10 mai 2018 (Ustawa o ochronie danych osobowych).

Acestea stabilesc norme clare privind modul în care trebuie tratate datele sensibile, în special datele care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase, apartenența sindicală, datele genetice, datele biometrice, datele privind sănătatea sau datele privind viața sexuală sau orientarea sexuală a unei persoane.

Oficiul pentru protecția datelor personale (UODO - Urząd Ochrony Danych Osobowych) este autoritatea națională de supraveghere. Acesta oferă orientări, tratează plângerile și are competența de a efectua audituri. UODO poate impune amenzi administrative de până la 20 de milioane EUR sau 4% din cifra de afaceri anuală globală a unei companii pentru încălcări grave ale GDPR.

Principiile cheie pentru protecție în Polonia sunt similare cu cele din alte țări. Remarcăm ca particularitate cerințe mai stricte privind consimțământul. Astfel, consimțământul trebuie să fie liber exprimat, specific, informat și **lipsit de ambiguitate**. În practică, aceasta înseamnă că pentru datele sensibile consimțământul trebuie să fie afirmat în mod explicit - de obicei prin semnătură scrisă sau digitală, nu doar prin bifarea unei căsuțe.

În Polonia, spitalele și clinicile trebuie să securizeze dosarele pacienților atât în temeiul GDPR, cât și al reglementărilor poloneze privind sănătatea; angajatorii pot prelucra date privind sănătatea sau cazierul judiciar numai în condiții stricte, de obicei cu o justificare legală dincolo de consimțământ. Școlile și universitățile trebuie să trateze cu mare atenție datele biometrice sau datele legate de sănătate, necesitând adesea îndrumarea sau aprobarea UODO. Marketingul sau crearea de profiluri bazate pe categorii sensibile (cum ar fi convingerile politice) sunt, în general, interzise fără consimțământ explicit.

SPANIA

La 17 februarie 2024, DSA a devenit pe deplin aplicabilă, impunând obligații platformelor online și serviciilor intermediare care operează în Spania. Deși direct aplicabilă, Spania poate introduce legislație națională complementară pentru a aborda aspecte specifice ale aplicării sale sau pentru a stabili mecanisme procedurale suplimentare. Până în aprilie 2025, Spania nu a adoptat o legislație națională specifică care să completeze Regulamentul UE 2022/2065 (DSA). De exemplu, au existat discuții cu privire la modificarea legilor existente, cum ar fi Legea 34/2002 privind serviciile societății informaționale și comerțul electronic (LSSI), pentru alinierea la cerințele DSA. Cu toate acestea, până în prezent, nu au fost oficializate astfel de modificări.

Comisia Națională a Piețelor și Concurenței (Comisión Nacional de los Mercados y la Competencia CNMC) a fost desemnată coordonator al serviciilor digitale (DSC) național la 24 ianuarie 2024. CNMC a fost numită DSC din Spania printr-o decizie oficială[13] a Ministerului spaniol pentru transformare digitală și servicii publice. Această desemnare împuternicește CNMC să monitorizeze respectarea DSA, să gestioneze plângerile utilizatorilor și să se coordoneze cu alte autorități naționale și ale UE pentru a asigura o aplicare coerentă a regulamentului.

În prezent, CNMC supraveghează, investighează și sancționează furnizorii de servicii care intră sub incidența DSA. În plus, CNMC are sarcina de a certifica agenții de semnalizare de încredere și de a colabora cu Agenția spaniolă pentru protecția datelor pentru a asigura respectarea reglementărilor privind protecția datelor.

În ciuda acestei desemnări, la 16 decembrie 2024, Comisia Europeană a emis un aviz motivat[14] adresat Spaniei pentru că nu și-a împuternicit pe deplin CSD, așa cum prevede DSA. Spaniei i s-au acordat două luni pentru a remedia aceste deficiențe. În iulie 2024, Comisia Europeană a inițiat procedura de încălcare a dreptului comunitar (infringement) împotriva Spaniei pentru că nu și-a împuternicit pe deplin coordonatorul serviciilor digitale (DSC), așa cum prevede Regulamentul privind serviciile digitale (DSA). Spaniei i s-au acordat două luni pentru a remedia aceste deficiențe. Până în aprilie 2025, nu există informații publice care să confirme că Spania a răspuns pe deplin preocupărilor Comisiei sau că procedura privind încălcarea dreptului comunitar a fost încheiată. Absența actualizărilor sugerează că este posibil ca Spania să fie încă în curs de punere în aplicare a măsurilor necesare pentru a-și abilita CSD în conformitate cu DSA. Nerespectarea avizului motivat ar putea determina Comisia să trimită cazul în fața Curții de Justiție a Uniunii Europene (CJUE) pentru acțiuni ulterioare.

În Spania, cerința de a furniza un act de identitate (ID) la înregistrarea pe o platformă online depinde de natura platformei și de serviciile pe care le oferă. Deși nu există o lege generală

[13] NdP-CNMC-DSA.pdf

[14] The Commission calls on Belgium, Bulgaria, Spain, The Netherlands and Poland to comply with the Digital Services Act | Shaping Europe's digital future

care să impună verificarea identității pentru toate platformele online, anumite sectoare și servicii au reglementări specifice.

Platformele online care oferă servicii financiare, cum ar fi serviciile bancare sau de investiții, sunt supuse reglementărilor privind cunoașterea clientelei (KYC) și combaterea spălării banilor (AML). Acestea impun platformelor să verifice identitatea utilizatorilor lor pentru a preveni frauda și a respecta obligațiile legale.

Platformele care oferă conținut sau servicii sensibile la vârstă pot solicita verificarea identității pentru a se asigura că utilizatorii îndeplinesc cerințele minime de vârstă. De exemplu, au existat discuții cu privire la creșterea vârstei minime pentru crearea de conturi de social media de la 14 la 16 ani, pentru a spori protecția minorilor online.

Accesarea platformelor guvernamentale oficiale necesită adesea o verificare solidă a identității. Spania utilizează sisteme precum Cl@ve, un sistem de identificare digitală care permite cetățenilor să se autentifice în mod sigur în cadrul diferitelor servicii publice. Înregistrarea pentru Cl@ve necesită verificarea prin metode cum sunt identificarea video sau confirmarea în persoană.

Gazdele care oferă cazare prin intermediul platformelor online sunt obligate să colecteze și să înregistreze datele de identificare ale clienților la autorități. Această obligație decurge din Decretul regal 933/2021, în vigoare de la 2 decembrie 2024, care impune colectarea de informații specifice privind oaspeții în scopuri de securitate.

Pentru majoritatea celorlalte platforme online, cum ar fi site-urile de comerț electronic, rețelele de socializare sau forumurile, nu există, în general, nicio obligație legală de a furniza un act de identitate în timpul înregistrării. Cu toate acestea, platformele individuale își pot implementa propriile procese de verificare pe baza politicilor lor sau pentru a spori securitatea și încrederea în cadrul serviciilor lor.

Legea organică 3/2018 privind protecția datelor și drepturile digitale (LOPDGDD) completează GDPR în Spania. Aceasta introduce norme specifice pentru prelucrarea datelor în domenii precum ocuparea forței de muncă, drepturile online ale minorilor și drepturile digitale (de exemplu, dreptul la deconectare digitală) și asigură garanții suplimentare pentru datele sensibile, solicitând adesea consimțământul explicit.

Agencia Española de Protección de Datos (AEPD) este autoritatea națională pentru protecția datelor. Aceasta gestionează plângerile, efectuează investigații și emite amenzi, oferă orientări și aplică atât GDPR, cât și LOPDGDD.

Câteva exemple de protecție în practică sunt faptul că spitalele trebuie să obțină consimțământul explicit pentru a stoca sau partaja dosarele medicale, sistemele biometrice de prezență (cum ar fi scanerele de amprente digitale) necesită o justificare strictă, școlile trebuie să obțină acordul părinților pentru a utiliza fotografiile elevilor sau pentru a colecta date biometrice, iar datele sensibile nu pot fi utilizate pentru crearea de profiluri de marketing sau publicitate fără consimțământ explicit.

În ianuarie 2025, AEPD a impus o amendă de 6,5 milioane EUR unui distribuitor de telecomunicații în urma unei încălcări semnificative a securității datelor cauzată de un atac ransomware. Încălcarea a expus date sensibile ale clienților, evidențiind eșecul companiei de a implementa măsuri de securitate adecvate.

În martie 2025, AEPD a amendat LaLiga cu 1 milion de euro pentru colectarea și prelucrarea necorespunzătoare a datelor biometrice ale spectatorilor prin intermediul sistemelor de recunoaștere facială de la intrarea în stadion. Această acțiune a fost considerată disproporționată și contrară GDPR. De asemenea, AEPD a dispus suspendarea acestor sisteme până la verificarea conformității.

UNGARIA

Parlamentul Ungariei a introdus în procedură specifică proiectul de lege de punere în aplicare a DSA, pentru a stabili cadrul juridic național necesar. Acest proiect legislativ definește norme specifice pentru serviciile de intermediere online care funcționează pe teritoriul Ungariei.

Regulamentul DSA se aplică furnizorilor de servicii de intermediere (ISP) stabiliți în Ungaria, precum și celor care nu sunt stabiliți în țară, dar oferă servicii în Ungaria. În special, aceasta se extinde dincolo de principiul țării de origine al DSA, afirmând aplicabilitatea la furnizorii ale căror servicii online sunt accesibile în Ungaria.

Legea CIV din 2023 privind anumite norme pentru furnizorii de servicii online desemnează Autoritatea Națională pentru Media și Comunicații (NMHH) drept principalul organism responsabil de supravegherea și aplicarea dispozițiilor DSA în Ungaria[15]. NMHH are sarcina de a se asigura că furnizorii de servicii digitale respectă reglementările stabilite.

Autoritatea Națională pentru Media și Comunicații (NMHH) este și organismul autonom de reglementare din Ungaria care supraveghează sectoarele media, comunicațiilor electronice și poștale. Printre competențele sale în domeniu se găsesc:

- Reglementarea și supravegherea mass-media: asigură conformitatea conținutului media cu legislația națională, inclusiv monitorizarea echilibrului politic și protecția minorilor; gestionează alocarea licențelor de radiodifuziune și a frecvențelor pentru serviciile de televiziune și radio; promovează educația mediatică prin Implicarea în activități de sensibilizare și alfabetizare mediatică a cetățenilor, cu accent pe protecția copiilor;
- Supravegherea comunicațiilor electronice: monitorizează respectarea de către furnizorii de telecomunicații a reglementărilor, protejând drepturile consumatorilor și promovând concurența loială; alocă și supraveghează utilizarea frecvențelor radio.

În conformitate cu DSA și cu măsurile de punere în aplicare ale Ungariei, furnizorii de servicii digitale sunt supuși mai multor obligații, inclusiv: moderarea conținutului (mecanisme de detectare și eliminare promptă a conținutului ilegal), furnizarea de informații clare privind practicile de publicitate și sistemele de recomandare a conținutului; protejarea utilizatorilor împotriva activităților dăunătoare și asigurarea respectării drepturilor lor online; colaborarea cu autoritățile naționale pentru abordarea riscurilor sistemice și respectarea măsurilor de investigare.

Nerespectarea poate duce la sancțiuni semnificative, subliniind importanța aderării platformelor la aceste reglementări.

---

[15] Într-o scrisoare adresată Comisiei Europene, 36 deputați europeni își exprimă temerea că încredințarea controlului platformelor online către NMHH, cunoscut pentru legăturile sale cu propaganda guvernamentală, ar putea încălca cerințele de independență ale DSA.
(...) alegerea de către Ungaria a NMHH a stârnit îngrijorări cu privire la potențiala influență externă. Scrisoarea subliniază importanța independenței DSC, în special în gestionarea plângerilor legate de moderarea conținutului și libertatea de exprimare. Deputații se referă, de asemenea, la preocupările legate de lipsa de independență a Consiliului pentru mass-media din Ungaria (Médiatanács), care face parte din NMHH. Scrisoarea solicită clarificări din partea Comisiei cu privire la respectarea de către NMHH a cerințelor de independență și propune monitorizarea atentă a nominalizărilor DSC pentru a asigura aderarea la principiile DSA. Hungary's appointed DSA authority raises concerns in Brussels | Digital Watch Observatory, MEPs concerned about Hungarian digital authority's lack of independence - Euractiv

În Ungaria, nu există nicio cerință legală generală care să oblige persoanele fizice să furnizeze documente de identificare atunci când se înregistrează pe platforme online. Cu toate acestea, anumite platforme sau servicii pot solicita verificarea identității în funcție de natura lor specifică, de reglementările din domeniu sau de politicile interne.

Pentru majoritatea serviciilor online, cum ar fi site-urile de comerț electronic sau platformele social media, legislația maghiară nu impune utilizatorilor să prezinte un act de identitate oficial în timpul înregistrării. Cu toate acestea, platformele își pot implementa propriile procese de verificare pe baza politicilor lor interne.
Tipurile de platforme specifice care solicită verificarea identității sunt:

- Serviciile guvernamentale: Accesarea serviciilor de e-guvernare din Ungaria necesită înregistrarea prin intermediul sistemului Client Gate - Ügyfélkapu. În cadrul acestui proces, persoanele trebuie să își verifice identitatea folosind documente oficiale, cum ar fi o carte de identitate, un pașaport sau un permis de ședere valabil. Înregistrarea poate fi efectuată personal la birourile desemnate sau online pentru cei care dețin o carte de identitate maghiară emisă după 1 ianuarie 2016.
- Înregistrarea societăților comerciale: Întreprinderile care își desfășoară activitatea în Ungaria trebuie să se înregistreze la Cégkapu, portalul întreprinderilor online care facilitează comunicarea electronică cu autoritățile. Înregistrarea necesită informații oficiale despre societate și este efectuată de obicei de reprezentantul legal al societății.
- Produse media online: editorii de produse media online sunt obligați să își înregistreze serviciile la Autoritatea Națională pentru Media și Comunicații (NMHH). Deși înregistrarea este obligatorie, aceasta nu este o condiție prealabilă pentru începerea operațiunilor și trebuie finalizată în termen de 60 de zile de la începerea serviciului.
- Anumite servicii profesionale: Platformele care oferă servicii specializate, cum ar fi portalurile de locuri de muncă, pot solicita întreprinderilor să furnizeze informații valide despre companie, inclusiv numere de identificare fiscală și date de contact oficiale, în timpul înregistrării. De exemplu, Profession.hu impune ca numai

întreprinderile înregistrate și persoanele care desfășoară activități independente să poată deschide conturi pentru a posta anunțuri de angajare.

În Ungaria, protecția datelor cu caracter personal sensibile - categorii speciale de date cu caracter personal - este reglementată în principal de Regulamentul general privind protecția datelor (GDPR) și de legea națională de punere în aplicare din Ungaria:
Prelucrarea tipurilor de date sensibile este interzisă, cu excepția cazului în care se aplică excepții specifice, cum ar fi consimțământul explicit, interesul vital, obligația legală sau interesul public substanțial.
Legea CXII din 2011 privind dreptul la autodeterminare informațională și libertatea de informare (Infotv.) completează GDPR și reglementează prelucrarea datelor de către organismele publice, stabilește Autoritatea națională pentru protecția datelor și libertatea de informare (NAIH) ca autoritate de supraveghere și cuprinde norme suplimentare privind securitatea, drepturile persoanelor vizate și gestionarea datelor guvernamentale.
Protecțiile esențiale pentru datele sensibile implică:

- Cerințe privind consimțământul explicit al persoanelor înainte de prelucrarea datelor lor sensibile solicitat de către operatorii de date, iar consimțământul trebuie să fie liber exprimat, informat și revocabil în orice moment;
- Măsuri de securitate a datelor care înseamnă că organizațiile trebuie să aplice măsuri de protecție tehnice și organizaționale adecvate, cum ar fi criptarea, controlul accesului și pseudonimizarea;
- Evaluări ale impactului asupra protecției datelor (DPIA) necesare înainte de inițierea oricărei prelucrări susceptibile de a prezenta un risc ridicat pentru drepturile individuale, în special atunci când sunt implicate date sensibile.

Rezidenții maghiari beneficiază de toate drepturile prevăzute de GDPR: acces și rectificare, ștergerea („dreptul de a fi uitat”), restricționarea prelucrării, portabilitatea datelor, dreptul la opoziție, dreptul de a nu fi supus procesului decizional automatizat.
Operatorii de date trebuie să notifice NAIH cu privire la încălcările securității datelor care implică date sensibile în termen de 72 de ore. În cazul în care încălcarea este susceptibilă să conducă la un risc ridicat pentru persoane, aceștia trebuie să informeze, de asemenea, persoanele afectate.

Autoritatea Națională pentru Protecția Datelor și Libertatea de Informare (NAIH) investighează plângerile și efectuează audituri, emite orientări și recomandări, poate impune amenzi de până la 20 de milioane EUR sau 4% din cifra de afaceri anuală globală.

Un exemplu de sancțiune impusă de NAIH este pentru utilizarea ilegală a analizei AI emoționale de către Budapest Bank. Între mai 2018 și septembrie 2021, Budapest Bank a utilizat un software de inteligență artificială pentru a analiza stările emoționale ale clienților în timpul apelurilor de service. Această prelucrare a implicat date biometrice sensibile fără un temei juridic valabil, fără o echilibrare adecvată a intereselor sau fără garanții adecvate. În plus, banca nu a informat clienții cu privire la această prelucrare a datelor și la drepturile lor, inclusiv dreptul de a se opune. În consecință, în 2022, NAIH a amendat Budapest Bank cu aproximativ 700 000 EUR pentru aceste încălcări ale GDPR. Banca a fost obligată să înceteze activitățile ilegale de prelucrare a datelor și să pună în aplicare măsuri pentru a asigura conformitatea cu reglementările privind protecția datelor.

În 2019, Digi, un important furnizor de servicii de comunicații electronice, a suferit o încălcare a securității datelor din cauza unei vulnerabilități nerezolvate în sistemul său de gestionare a conținutului. Această încălcare a expus date personale și sensibile, inclusiv date de identificare, adrese de e-mail, numere de telefon și numere de cont bancar, care ar fi putut duce la furtul identității. NAIH a impus Digi o amendă de 100 de milioane HUF (aproximativ 285 000 EUR) pentru că nu a pus în aplicare măsuri tehnice și organizatorice adecvate pentru a proteja datele cu caracter personal. Digi a abordat vulnerabilitatea prin aplicarea patch-urilor necesare și prin îmbunătățirea măsurilor de securitate a datelor pentru a preveni incidente viitoare.

WEBOGRAFIE

General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679

Digital Services Act (DSA) – Regulation (EU) 2022/2065

eIDAS Regulation – Regulation (EU) No 910/2014

Guidelines on the Right to Data Portability (GDPR)

Digital Identity for the EU (European Digital Identity Wallet)

"The Impact of GDPR on Digital Platforms"

"Online Identity Verification in the EU: Balancing Security and Privacy"