

Către:	UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA
În vederea:	CONGRESULUI AVOCAȚILOR 2025
În atenția:	Domnului Președinte, Prof.univ.dr., Avocat Traian C. BRICIU

Subsemnata **Spătaru G. Mădălina**, în calitate de responsabil cu protecția datelor externalizat la nivelul Uniunii Naționale a Barourilor din România („UNBR”) prezintă în cele ce urmează

**Raportul de activitate
al
Responsabilului cu Protecția Datelor („DPO”)
privind
activitatea de conformarea a UNBR cu prevederile aplicabile în materia protecției datelor cu caracter personal**

Capitolul I. CONTEXT

Colaborarea dintre UNBR și Spătaru G. Mădălina a fost inițiată având în vedere lansarea proiectului privind acordarea accesului și prelucrarea datelor cu caracter personal din Registrul Național de Evidență a Persoanelor al Direcției Generale pentru Evidența Persoanelor, în scopul obținerii de către avocați a datelor cu caracter personal necesare îndeplinirii atribuțiilor legale de asigurare a accesului justițiabililor la justiție într-un termen rezonabil și de acordare a asistenței juridice, precum și în scopul actualizării de către barourile membre ale UNBR a tabloului avocaților și a gestionării în bune condiții a Fondului de pensii și alte drepturi de asigurări sociale ale avocaților.

Pe fondul colaborării în acest scop inițial, s-a identificat oportunitatea actualizării măsurilor, procedurilor și proceselor existente la nivelul UNBR pentru asigurarea protecției datelor cu caracter personal, inclusiv din perspectiva informării adecvate referitor la activitățile de prelucrare desfășurate și gestionarea adecvată a solicitărilor persoanelor vizate.

Având în vedere acest context, s-a stabilit un plan de măsuri de remediere la nivelul UNBR, ce are în vedere principalele proceduri și măsuri necesare a fi implementate pentru minimizarea riscurilor în ceea ce privește prelucrarea datelor cu caracter personal.

RAPORT PROTECȚIA DATELOR CU CARACTER PERSONAL

Suplimentar, din perspectivă contractuală, s-a recurs la o analiză a contractelor în vigoare la nivelul UNBR, ce implică o componentă de prelucrare a datelor cu caracter personal și actualizarea acestora astfel încât să se asigure controlul asupra datelor cu caracter personal prelucrate, precum și stabilirea în mod clar a drepturilor și obligațiilor părților contractuale astfel încât acestea să se asigure gestionarea corectă și legală a datelor cu caracter personal.

Totodată, având în vedere că informarea adecvată a persoanelor vizate reprezintă o condiție *sine qua non* pentru asigurarea conformității cu prevederile aplicabile în materia protecției datelor cu caracter personal s-a recurs, fie la actualizarea notelor de informare existente, fie la implementarea unor noi note de informare, pentru noi activități de prelucrare, cum ar fi, spre exemplu, Nota de informare aplicabilă în cadrul parteneriatului cu Ambasada Statelor Unite ale Americii la București, pentru asigurarea priorității pentru avocați în procesul de obținere a vizei temporare B1/B2 pentru acordarea accesului pe teritoriul Statele Unite ale Americii.

În același timp, având în vedere calitatea UNBR de organ reprezentativ și deliberativ al barourilor din România, ce rezolvă probleme interesând profesia de avocat, s-a stabilit oportunitatea creșterii conștientizării în rândul avocaților cu privire la importanța asigurării protecției datelor cu caracter personal, inclusiv în contextul utilizării în continuă creștere a sistemelor de inteligență artificială, prin elaborarea unui Ghid de bune practici, de avut în vedere de către avocați.

Capitolul II. MĂSURI IMPLEMENTATE

Obligații de informare
- Implementare notă de informare pentru avocați privind accesul la Registrul Național de Evidență a Persoanelor - Implementare notă de informare pentru justițiabili privind accesul la Registrul Național de Evidență a Persoanelor - Implementare notă de informare privind parteneriatului cu Ambasada Statelor Unite ale Americii la București, pentru asigurarea priorității pentru avocați în procesul de obținere a vizei temporare B1/B2 pentru acordarea accesului pe teritoriul Statele Unite ale Americii - Actualizarea notei de informare pentru platforma ifep.ro - Actualizarea notei de informare pentru accesarea fondului de solidaritate - Actualizare notă de informare și cerere de acces ANCPI
Obligații contractuale
- Implementare acord de confidențialitate pentru gestionarea activității de acces la Registrul Național de Evidență a Persoanelor - Implementare acord de prelucrarea a datelor cu caracter personal privind implementarea platformei ifep.ro

RAPORT PROTECȚIA DATELOR CU CARACTER PERSONAL

- Implementare acord de prelucrarea a datelor cu caracter personal privind implementarea modulului Registry
- Implementare act adițional privind execuția de carduri CCBE
- Asigurarea unui instructaj adecvat pentru angajații cu atribuții în gestionarea activității de acces la Registrul Național de Evidență a Persoanelor
- Implementarea unui regulament de acces la Registrul Național de Evidență a Persoanelor
- Efectuarea unei analize privind necesitatea actualizării cadrului contractual existent între UNBR și ANCPPI

Proceduri și procese

- Implementarea unei proceduri privind gestionarea solicitărilor de ștergere a datelor cu caracter personal din platforma ifep.ro
- Implementarea unui registru de evidență al activităților de prelucrare desfășurate ca urmare a acordării accesului la Registrul Național de Evidență a Persoanelor
- Implementarea unei proceduri privind gestionarea solicitărilor persoanelor vizate pentru activităților de prelucrare desfășurate ca urmare a acordării accesului la Registrul Național de Evidență a Persoanelor
- Derularea unei evaluări de impact cu privire la protecția datelor cu caracter personal pentru activitățile de prelucrare desfășurate ca urmare a acordării accesului la Registrul Național de Evidență a Persoanelor

Capitolul III. GESTIONAREA SITUAȚIEI OCAZIONATE CU PLATFORMA IFEP.RO

În data de 05 ianuarie 2024, utilizând platforma informatică a domeniului incorpo.ro, deținut de societatea ENTRYRISE S.R.L., au fost transmise de pe adresa de e-mail alexandra.ardelean@incorpo.ro e-mailuri semnate de administratorul societății, către un număr important de avocați (se estimează peste 30.000 de e-mailuri), pe adrese de e-mail, în care se pretinde că au fost obținute o serie de informații din baza de date aferentă platformei ifep.ro (CNP, număr de telefon, număr de legitimație / card avocat CCBE) prin utilizarea unui „*endpoint accesibil fără parolă, și indexat de Google.*” Se susținea în e-mail că „*acest endpoint a fost accesibil pentru aproximativ 2 ani*”, însă nu sunt deținute „*informații clare*”. În cuprinsul e-mailului se arată că „*a fost notificat IFEP în mod direct pe adresa de mail din termenii și condițiile pentru a rectifica problema*” și că „*deși s-a rectificat în aceiași zi, avocații nu au fostificați de existența breșei*”. Se recomandă în e-mail citirea „*comunicatului de presă al Incorpo.ro referitor la breșa de securitate al IFEP*”. Nu în ultimul rând, în partea finală a e-mailului se arată faptul că avocatul care dorește o probă cu privire la existența breșei este rugat să transmită prin e-mail la adresa office@incorpo.ro un document semnat electronic prin care să solicite expres și să furnizeze totodată societății ENTRYRISE S.R.L. care deține platforma domeniului incorpo.ro dreptul/acordul de procesare al datelor respective pentru a transmite avocatului totalitatea datelor obținute.

RAPORT PROTECȚIA DATELOR CU CARACTER PERSONAL

În același timp, societatea ENTRYRISE S.R.L. a publicat un comunicat¹ din care a rezultat o suspiciune rezonabilă că datele cu caracter personal aparținând a aproximativ 30.000 de avocați se regăsesc pe infrastructura informatică a societății ENTRYRISE S.R.L., în mod neautorizat.

Aceste acțiuni au stârnit îngrijorare în rândul avocaților, iar UNBR, în calitate de organ reprezentativ și deliberativ al barourilor din România, ce rezolvă probleme interesând profesia de avocat, astfel cum este reglementat prin Legea nr. 51/1995 pentru organizarea și exercitarea profesiei de avocat, a lansat o investigație amplă referitor la cele de mai sus.

Investigația a presupus interogarea tuturor registrelor informatice existente la nivelul ifep.ro, prin:

- Verificarea codului sursă aferent endpoint-ului menționat ca fiind vulnerabil;
- Verificarea codului sursă aferent tuturor interfețelor, procedurilor stocate;
- Verificarea evenimentelor existente pe server;
- Verificarea corespondenței.

Au fost de asemenea luate următoarele măsuri de răspuns imediat:

Din punct de vedere tehnic

- Efectuare verificări cu privire la elementele apărute în spațiul public în vederea identificării potențialei breșe de securitate la care s-a făcut referire;
- Evaluarea tehnică amănunțită a codului sursă pe aspectele tehnice precizate în spațiul public, respectiv endpointul <https://www.ifep.ro/Ws/InternalWebServices.asmx>, a tuturor dependențelor acestuia și a interfețelor unde este utilizat, pentru a vedea dacă se susțin informațiile apărute în spațiul public;
- Verificarea altor aspecte specifice codului sursă ce ar fi putut intra în categoria breșei de securitate menționate;
- Verificarea integrității bazei de date;
- Verificarea sistemului de operare (jurnale);
- Verificarea existenței pachetelor noi de actualizare ale sistemului de operare și ale aplicațiilor instalate și analiza impactului acestora;
- Actualizarea pachetelor nuget (bibliotecile folosite în portal) la ultimele versiuni, unde a fost posibil;

¹ https://www.incorpo.ro/ro-ro/press/ifep-data-breach/?utm_nooverride=1&utm_source=sntp&utm_medium=newsman&utm_campaign=SMTP-20240105

RAPORT PROTECȚIA DATELOR CU CARACTER PERSONAL

- Înlocuirea unor pachete nuget cu unele mai eficiente;
- Actualizarea codului sursă prin adăugarea unor elemente de jurnalizare a endpoint-ului la care s-a făcut referire în breșa de securitate;
- Implementarea pe serverul de email a unui script care transmite pe mail-ul helpdesk@ifep.ro în mod automat, în fiecare săptămână, a tuturor jurnalelelor corespondenței;
- Inițierea unui proces de evaluare tehnică amănunțită a tuturor interfețelor existente în portal, a structurii bazei de date, a procedurilor stocate pentru a identifica dacă există vreo vulnerabilitate ce ar fi putut fi exploataată prin: injectare SQL (SQL injection), cross-site scripting (CSS), cross-site request forgery (CSRF), buffer overflow, injecție comenzi, expunere date sensibile, vulnerabilități ale bibliotecilor cu impact asupra portalului, atacuri MitM (man-in-the-middle), verificarea elementelor de securitate aferente autentificării și gestionării sesiunilor, configurările de securitate, validarea și sanitizarea inputurilor, deserializarea datelor cu posibilitate de rulare cod arbitrar, analiza algoritmilor criptografici pentru a identifica nivelul de protecție și nivelul de actualitate, atacuri Denial of Service (DoS) și Distributed Denial of Service (DDoS) precum și alte vulnerabilități ce ar putea fi identificate în urma analizei;
- verificarea corespondenței pentru a vedea dacă se susțin elementele lansate în spațiul public informațiile privind potențiala breșă de securitate.

Din punct de organizatoric

- Comunicarea continuă și eficientă între UNBR și societatea Intra Connect S.R.L. (în calitate de persoană împuternicită);
- Formularea de răspunsuri prompte la solicitările de informații ale avocaților;
- Formularea de răspunsuri prompte la solicitările de exercitare a drepturilor emise de avocați;
- Emiterea unui comunicat transparent² privind rezultatul investigațiilor interne și următorii pași de gestionare a situației;
- Transmiterea unei sesizări către ANSPDCP privind situația ocazionată. Pentru claritate, această sesizare a avut în vedere atragerea atenției autorității de supraveghere cu privire la acțiunile întreprinse de ENTRYRISE S.R.L. și administratorul său. Până la acest moment, nu am primit actualizări din partea autorității de supraveghere.
- Furnizarea de răspunsuri asupra întrebărilor transmise de ANSPDCP cu privire la pretinsa breșă de securitate.

Ca urmare a investigației interne desfășurate, s-a concluzionat că nu a fost identificată nicio breșă de securitate de tipul celei reclamate în spațiul public.

² <https://www.unbr.ro/comunicat-al-comisiei-permanente-a-unbr-referitor-la-informatiile-aparute-in-spatiul-public-cu-privire-la-o-pretinsa-bresa-de-securitate-a-platformei-ifep/>

RAPORT PROTECȚIA DATELOR CU CARACTER PERSONAL

În același timp, UNBR a sesizat ANSPDCP cu privire la deținerea unor date cu caracter personal, făcută public prin comunicatul și e-mailul transmis, în vederea atragerii atenției autorității de supraveghere asupra anumitor prelucrări ilegale de date ce ar fi putut fi săvârșite de către terțul în discuție.

Capitolul IV. MĂSURI IMPLEMENTATE CU PRIVIRE LA ACTIVITATEA CURENTĂ A UNBR

Raportat la specificul activității UNBR, au fost identificate următoarele necesități, care și-au găsit soluționarea prin următoarele măsuri implementate:

- Ca urmare a primirii unui număr considerabil de solicitări de ștergere a datelor cu caracter personal cu referire la datele cu caracter personal prelucrate prin intermediul IFEP, a fost implementată o procedură de ștergere a datelor care să asigure claritate și celeritate în soluționarea cererilor, ce are în vedere diferite tipuri de scenarii (e.g. avocat activ/străin/suspendat), actorii implicați, sarcinile alocate și timpul de răspuns;
- În același timp, a fost implementat un registru al solicitărilor persoanelor vizate, necesar pentru a menține evidența oricăror cereri ce parvin cu privire la exercitarea drepturilor în materia protecției datelor cu caracter personal, pentru a asigura că aceste solicitări sunt soluționate în termenele legale;
- Formularea de răspunsuri asupra solicitărilor de ștergere a datelor cu caracter personal, gestionarea și coordonarea persoanelor implicate, în vederea respectării prevederilor legale;
- Menținerea relației cu persoanele vizate și formularea de răspunsuri la adresele primite din partea acestora, fie având în vedere conformarea cu obligațiile de informare cf. GDPR, fie raportat la exercitarea drepturilor prevăzute de regulamentul european;
- Pseudonimizarea la cerere a datelor cu caracter personal prelucrate, în baza prevederilor GDPR;
- Actualizarea permanentă a politicilor și procedurilor specifice din cadrul UNBR, pentru a răspunde noilor cerințe în ceea ce privește prelucrarea datelor cu caracter personal;
- În același timp, UNBR, în calitate de operator al datelor cu caracter personal, potrivit art. 17 alin. (2) din GDPR, a luat măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal;
- Formularea de răspunsuri la solicitările punctuale cu privire la datele cu caracter personal, în vederea respectării prevederilor legale aplicabile.

Capitolul V. MĂSURI SPECIFICE

RAPORT PROTECȚIA DATELOR CU CARACTER PERSONAL

A. Ca urmare a identificării necesității acordării accesului la date cu caracter personal prelucrate de Direcția Generală pentru Evidența Persoanelor („**D.G.E.P.**”) prin Registrul Național de Evidență a Persoanelor („**R.N.E.P.**”) și a încheierii Contractului Cadru dintre UNBR și DGEP, potrivit prevederilor legale aplicabile a fost efectuată o Evaluare a impactului asupra protecției datelor în contextul operațiunilor de prelucrare realizate cu ocazia desfășurării activității de accesare și prelucrare a datelor din Registrul Național de Evidență a Persoanelor al Direcției Generale pentru Evidența Persoanelor.

Această evaluare a presupus analizarea amănunțită a elementelor ce alcătuiesc ecosistemul prelucrării datelor cu caracter personal privind accesul la R.N.E.P., având în vedere, spre exemplu, scopul, modalitățile de prelucrare și măsurile tehnice și organizatorice implementate, pentru a asigura că prelucrarea datelor cu caracter personal se desfășoară în condiții de legalitate și securitate.

B. Actualizarea documentelor ce privesc accesarea R.N.E.P. (Registrul de evidență, regulamentul, notele de informare), astfel încât să acomodeze rezultatul Evaluării de impact;

C. Implementarea unei noi note de informare pentru platforma IFEP, prin care să se asigure respectarea principiului transparenței și a art. 12 și 13 din GDPR, precum și clarificarea calității din punctul de vedere al protecției datelor cu caracter personal a UNBR și Intra Connect S.R.L. (operator-persoană împuternicită).

Capitolul VI. MĂSURI ÎN CURS DE IMPLEMENTARE

Nr. crt.	Deficiența identificată	Risc posibil	Măsura propusă	Compartimente	Specificații/Status
1.	Registrul privind activitățile de prelucrare existente la nivelul UNBR	Încălcare art. 30 din GDPR	Redactarea și implementarea unui registru general privind activitățile de prelucrare existente la nivelul UNBR. Registrul va fi actualizat periodic, raportat la noile activități de prelucrare/noile proiecte implementate de UNBR	Secretariat Compartiment Protecția Datelor	Este implementat un registru specific privind accesul la RNEP. Este necesară redactarea și implementarea unui registru general care să acopere toate activitățile de prelucrare.

RAPORT PROTECȚIA DATELOR CU CARACTER PERSONAL

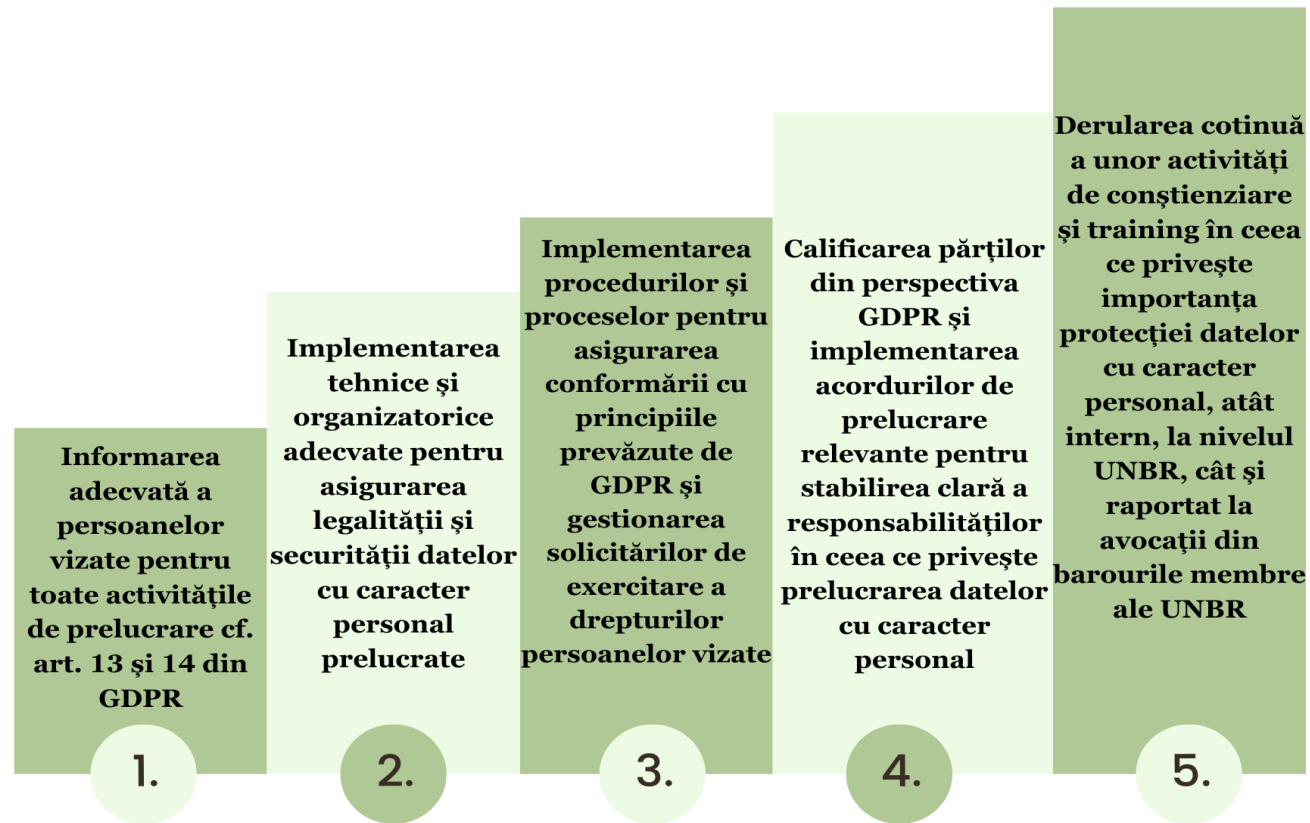
					Actualizare: Registrul a fost implementat.
2.	Procedura generală de gestionare a cererilor persoanelor vizate	Încălcare Capitolul III din GDPR și art. 32 din GDPR	Redactarea și implementarea de proceduri pentru a asigura că drepturile persoanelor vizate sunt respectate	Secretariat Compartiment Protecția Datelor	Este implementată o procedură specifică de gestionare a cererilor persoanelor vizate privind accesul la RNEP. Este necesară redactarea și implementarea unei proceduri generale privind gestionarea cererilor persoanelor vizate. Actualizare: Procedură redactată.
3.	Procedura privind gestionarea incidentelor de securitate	Încălcare art. 32 și 33-34 din GDPR	Redactarea și implementarea procedurii privind (i) acțiunile necesare a fi întreprinse în cazul unui incident de securitate, (ii) termenele de răspuns (iii) persoanele/departamentele responsabile	Secretariat Compartiment Protecția Datelor	Este necesară redactarea și implementarea unei proceduri privind gestionarea incidentelor de securitate pentru asigurarea unui răspuns imediat și eficient cu privire la orice breșe/suspiciuni referitoare la existența unor breșe. Actualizare: Procedură redactată.

RAPORT PROTECȚIA DATELOR CU CARACTER PERSONAL

4.	Procedura care sa reglementeze fluxul și arhivarea datelor cu caracter personal (fie electronic, fie fizic)	Încălcare art. 5 și 32	Redactarea și implementarea procedurii privind fluxul și arhivarea documentelor ce conțin date cu caracter personal la nivelul UNBR (fie electronic, fie fizic)	Secretariat Compartiment Protecția Datelor	Este necesară implementarea unei astfel de proceduri care să asigure condițiile în care documentele ce conțin date cu caracter personal, atât în format electronic, cât și fizic
5.	Notele de informare implementate la nivelul UNBR	Încălcare art. 12, 13 și 14	Revizuirea notelor de informare implementate la nivelul UNBR pentru a cuprinde totalitatea informațiilor prevăzute de art. 12, 13 și 14 din GDPR, precum și pentru asigurarea respectării principiului transparenței	Secretariat Compartiment Protecția Datelor	Actualizare: Nota de informare aplicabilă IFEP a fost implementată.
6.	Derulare training	Încălcare art. 32	Este necesară derularea periodică de training-uri cu personalul din cadrul UNBR ce gestionează documente care conțin date cu caracter personal în vederea conștientizării importanței protecției datelor cu caracter personal și a familiarizării cu noțiunile aplicabile în materie	Toate compartimentele	Actualizare: Training in curs de a fi desfășurat.

Capitolul VII. OBIECTIVE

**Obiective în materia protecției datelor
cu caracter personal la nivelul UNBR**



Capitolul VIII. CONCLUZII

UNBR acordă o atenție sporită protecției datelor cu caracter personal, înțelegând că procesul de conformare reprezintă o activitate continuă, ce presupune convergența a multiple structuri.

Activitatea de conformare cu GDPR și de respectare a protecției datelor cu caracter personal presupune un efort constant, în care toate structurile să conștientizeze rolul și atribuțiile aplicabile, în vederea întăririi încrederii referitor la asigurarea protecției datelor la nivelul UNBR.

Importanța unor procese și proceduri corect implementate și asimilate la nivelul UNBR asigură atât *(i)* derularea de activități de prelucrare în legalitate, conform cu principiile și prevederile statuate de legislația și recomandările aplicabile la nivel european și național, cât și *(ii)* răspunsuri prompte la orice potențiale incidente.

Activitatea UNBR urmărește în vedere respectarea tuturor principiilor statuate de GDPR în îndeplinirea atribuțiilor de organ reprezentativ și deliberativ al barourilor din România, ce rezolvă probleme interesând profesia de avocat.

În acest sens, eforturile UNBR de asigurare a unei conștientizări sporite în ceea ce privește respectarea prevederilor în materia protecției datelor cu caracter personal continuă și se intensifică, în special în contextul utilizării la scară largă a noilor tehnologii, inclusiv a sistemelor de inteligență artificială.