ROMÂNIA
AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Bld.Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poștal 010336, București ; Tel: +40 31 805 9211; Fax: +40 31 805 9602 www.dataprotection.ro e-mail: ansdcp@dataprotection.ro

SENAT
BIROUL PERMANENT
Nr. 2191 Data 7.9.2026

SENATUL ROMÂNIEI
Nr.II 7190 / 03-09-2026

**Stimate Domnule Președinte,**

Am deosebita onoare de a supune atenției dumneavoastră Raportul de activitate aferent anului 2025, în conformitate cu dispozițiile art. 5 din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

**Cu aleasă prețuire,**

**Presedinte,**

**Ancuța Gianina OPRE**

**Domnului Mircea ABRUDEAN, Președintele Senatului**

**SENATUL ROMÂNIEI**

Digitally signed by
ANSPDCP
Date: 2026.08.31 13:32:55

# AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

# RAPORT ANUAL

## 2025

Raportul de activitate este transmis Senatului României, Camerei Deputaților, Guvernului României, Comisiei Europene și Comitetului European pentru Protecția Datelor, în temeiul prevederilor art. 5 din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

București

## CUVÂNT ÎNAINTE

***Stimate Domnule Președinte al Senatului,***

***Stimați Senatori,***

Am deosebita onoare de a prezenta, în fața Senatului României, Raportul de activitate aferent anului 2025 al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Din perspectiva protecției datelor cu caracter personal, în anul 2025 ritmul transformării digitale a continuat să genereze noi evoluții și provocări, care au implicat alte responsabilități pentru instituții și companii.

Datele cu caracter personal sunt parte integrantă și inerentă a tuturor activităților economice și sociale, iar dezvoltarea accelerată a soluțiilor tehnologice, utilizarea pe scară largă a serviciilor digitale și apariția unor noi modalități de analiză și valorificare a informațiilor impun o atenție constantă asupra modului în care aceste date sunt colectate, utilizate și protejate de fiecare entitate.

În acest context, activitatea de supraveghere desfășurată de instituția noastră a urmărit respectarea principiilor esențiale ale protecției datelor, precum legalitatea, transparența, proporționalitatea și limitarea utilizării datelor la scopurile pentru care acestea sunt colectate. Controalele desfășurate în sectorul public și privat au vizat atât identificarea unor eventuale deficiențe, cât și determinarea operatorilor să adopte măsuri concrete pentru îmbunătățirea modalităților de prelucrare și a metodelor de protejare.

Din această perspectivă, în anul 2025 activitatea Autorității a avut în vedere atât intervenția în situațiile în care au fost constatate încălcări ale legislației, cât și consolidarea unei culturi a responsabilității în materia protecției datelor. Informarea și responsabilizarea celor care prelucrează date cu caracter personal au reprezentat, astfel, componente importante ale demersurilor susținute ale instituției noastre.

Un segment important al activității desfășurate în această perioadă l-a constituit soluționarea plângerilor și sesizărilor formulate de persoanele fizice.

Acestea reprezintă, în mod direct, expresia preocupării cetățenilor pentru protejarea propriilor date și pentru exercitarea efectivă a drepturilor conferite de legislația în materie.

La nivel european, cooperarea dintre autoritățile de supraveghere a rămas esențială, în special în contextul prelucrărilor dintre statele membre ale Uniunii Europene, care împărtășesc același nivel înalt de protecție a datelor personale. Participarea instituției noastre la activitatea Comitetului European pentru Protecția Datelor a contribuit la schimbul de experiență și la dezvoltarea unei practici unitare în aplicarea normelor europene.

Rezultatele anului 2025 trebuie privite și prin raportare la resursele de care instituția noastră a dispus, având în vedere că, în pofida limitărilor bugetare și a insuficienței personalului specializat, Autoritatea a urmărit îndeplinirea atribuțiilor sale cu responsabilitate și cu orientare predilectă către sectoarele în care riscurile pentru drepturile persoanelor au fost semnificative.

Pentru perioada următoare, obiectivul nostru este ca activitatea de supraveghere să fie adaptată permanent realităților tehnologice și sociale aflate într-o continuă schimbare. Vom acorda în continuare atenție domeniilor în care utilizarea datelor personale generează riscuri sporite, concomitent cu consolidarea dialogului cu operatorii și cu continuarea informării publicului larg. Considerăm că dezvoltarea durabilă a societății digitale presupune încredere, iar încrederea poate fi construită numai atunci când persoanele au garanția că informațiile care le privesc sunt utilizate în mod legal, responsabil și transparent.

În încheiere, aș dori să vă mulțumesc pentru sprijinul acordat Autorității Naționale de Supraveghere și pentru atenția constantă în protejarea dreptului fundamental la viață privată, într-o societate aflată într-un proces continuu de transformare.

Vă asigur că vom continua să ne îndeplinim misiunea cu profesionalism și responsabilitate, astfel încât dreptul la protecția datelor cu caracter personal să aibă efectivitate și consistență, în considerarea necesității ca evoluția tehnologică actuală să fie însoțită de respectarea drepturilor și libertăților fundamentale ale persoanei fizice.

**Ancuța Gianina OPRE,**

**PREȘEDINTE**

# CUPRINS

**CAPITOLUL I**

**PREZENTARE GENERALĂ**.....pag. 5

**CAPITOLUL II**

**ACTIVITATEA DE AVIZARE, CONSULTARE, REPREZENTARE ÎN INSTANȚĂ ŞI INFORMARE PUBLICĂ**

**Secţiunea 1** Avizarea actelor normative.....pag. 8
**Secţiunea a 2-a** Puncte de vedere.....pag. 30
**Secţiunea a 3-a** Activitatea de reprezentare în instanță.....pag. 50
**Secţiunea a 4-a** Informare publică .....pag. 64

**CAPITOLUL III**

**ACTIVITATEA DE MONITORIZARE ŞI CONTROL**

**Secţiunea 1** Prezentare generală.....pag. 70
**Secţiunea a 2-a** Investigații din oficiu.....pag. 74
**Secţiunea a 3-a** Activitatea de soluționare a plângerilor.....pag. 96

**CAPITOLUL IV**

**ACTIVITĂŢI ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE**.....pag. 127

**CAPITOLUL V**

**MANAGEMENTUL ECONOMIC AL AUTORITĂŢII**.....pag. 137

## CAPITOLUL I

## PREZENTARE GENERALĂ

Raportul de activitate aferent anului 2025 al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea națională de supraveghere) este structurat pe cinci capitole, astfel:

**Capitolul I** prezintă o sinteză structurată a principalelor activități prin care Autoritatea națională de supraveghere și-a exercitat competențele legale specifice, astfel încât să fie evidențiate liniile strategice de intervenție.

Având în vedere obiectivului central al instituției referitor la asigurarea respectării normelor privind protecția datelor, reliefăm faptul că acțiunile desfășurate au vizat, în mod prioritar, monitorizarea și verificarea aplicării principiilor de prelucrare, consolidarea nivelului de informare a operatorilor și publicului, precum și continuarea cooperării cu autoritățile naționale și europene.

În **Capitolul al II-lea** sunt prezentate, într-o manieră structurată, activitățile de avizare, autorizare și consiliere derulate de Autoritatea națională de supraveghere, în exercitarea atribuțiilor conferite de Regulamentul (UE) 2016/679 și de cadrul normativ național aplicabil. Secțiunea evidențiază analiza proiectelor de acte normative primite, emiterea de avize și puncte de vedere privind aplicarea corectă a dispozițiilor legale în materia protecției datelor, precum și activitățile de informare publică desfășurate în sprijinul operatorilor și al persoanelor vizate.

În perioada analizată, instituția a formulat un număr semnificativ de avize privind acte normative și propuneri legislative, opinii și puncte de vedere, reflectând complexitatea situațiilor supuse evaluării și diversitatea domeniilor în care prelucrarea datelor ridică provocări specifice.

Așadar, remarcăm și în acest an menținerea unui interes ridicat din partea operatorilor din domeniul public și privat, precum și a persoanelor fizice, pentru aplicarea

adecvată a reglementărilor în vigoare. Aceștia au solicitat frecvent clarificări privind aplicabilitatea Regulamentului (UE) 2016/679 în situații cu implicații deosebite, ceea ce confirmă necesitatea continuării activităților de consiliere și îndrumare.

În același timp, în această secțiune sunt disponibile informații relevante privind cele mai importante litigii finalizate pe parcursul anului 2025, în care a fost implicată cu succes Autoritatea națională de supraveghere.

**Capitolul al III-lea** cuprinde o prezentare succintă a activității de control desfășurate în anul 2025, raportat la investigațiile efectuate, însoțite de principalele date statistice.

În ceea ce privește investigațiile din oficiu, acestea au urmărit modul în care au fost respectate prevederilor legale ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal și a sesizărilor primite de Autoritatea națională de supraveghere.

Referitor la incidentele de securitate notificate, precizăm că acestea au vizat, ca și în anii anteriori, pierderea confidențialității și accesul neautorizat a datelor cu caracter personal inclusiv în mediul online, măsurile de asigurare a securității și confidențialității datelor cu caracter personal, accesul neautorizat la sistemele informatice ale operatorilor, divulgarea neautorizată a datelor cu caracter personal.

În ceea ce privește soluționare a plângerilor și a sesizărilor, menționăm că, în anul 2025, au fost reclamate, în principal, aspecte privind încălcarea drepturilor persoanelor vizate, a principiilor de prelucrare a datelor, dezvăluirea datelor cu caracter personal către terți în spațiul public, în mediul online, primirea de mesaje comerciale nesolicitate, prelucrarea imaginilor prin intermediul sistemelor de supraveghere video de către persoane fizice și persoane juridice.

În același timp, în cadrul acestui capitol, sunt prezentate sancțiunile aplicate și măsurile corective dispuse în cadrul investigațiilor efectuate, dar și cazuri relevante din controalele realizate. Precizăm că și în cursul anului 2025, au fost aplicate amenzi și dispuse măsuri corective, într-o manieră similară anilor anteriori, în scopul remedierii activității operatorilor.

**Capitolul al IV-lea** conține principalele elemente din activitatea de relații externe a Autorității naționale de supraveghere, prin prezentarea documentelor adoptate la nivelul organismelor Uniunii Europene, cu aplicabilitate în domeniul protecției datelor personale.

În același timp, activitatea de cooperare cu alte autorități de supraveghere din Uniunea Europeană în vederea asigurării asistenței reciproce pentru a pune în aplicare Regulamentul (UE) 2016/679, este evidențiată, alături și aspecte pertinente privind contribuția instituției noastre în relația forurile europene.

**Capitolul al V-lea** conține informații semnificative privind managementul economic al instituției, veniturile și cheltuielile aferente, relevante din perspective resurselor bugetare limitate din anul 2025.

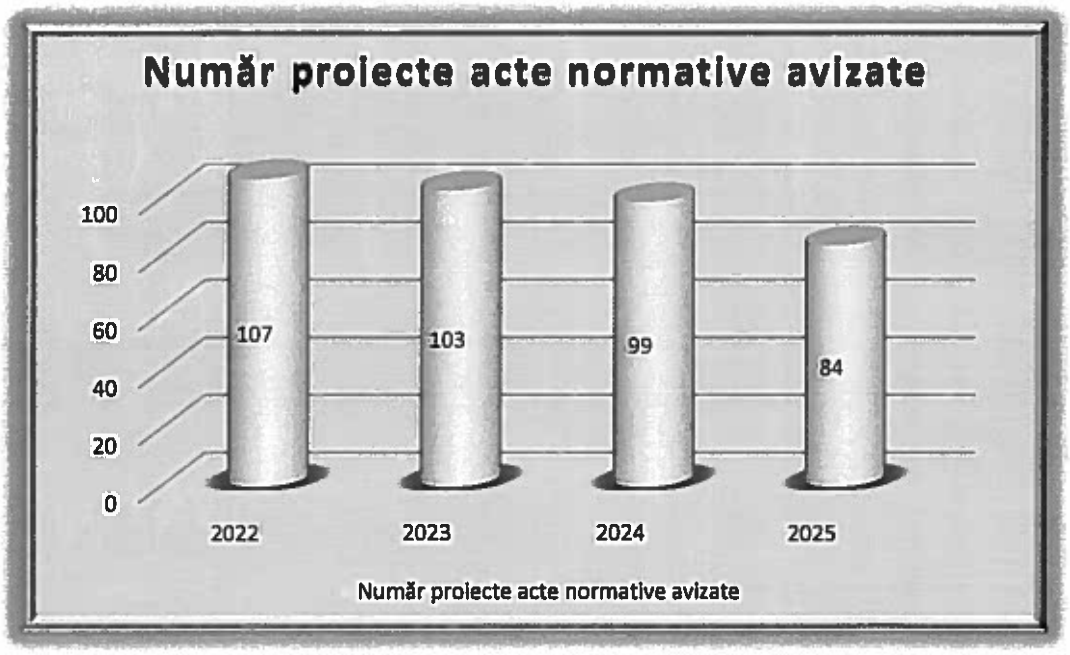
**Având în vedere aspectele prezentate în cadrul fiecărui capitol, raportat la obiectivele Autorității naționale de supraveghere, la resursele umane și financiare limitate, evidențiem că personalul instituției noastre a făcut eforturi deosebite pentru ca activitatea din anul 2025 să se desfășoare în parametri corespunzători.**

**În perspectivă, instituția noastră va urmări consolidarea activităților de monitorizare și control al operatorilor, soluționarea plângerilor și sesizărilor primite, precum și continuarea activităților de informare a publicului larg, în scopul asigurării unei aplicări eficiente și unitare a Regulamentului (UE) 2016/679 și a celorlalte acte normative incidente în materia protecției datelor cu caracter personal, în limita resurselor umane și financiare disponibile.**

# CAPITOLUL II
# ACTIVITATEA DE AVIZARE, CONSULTARE, REPREZENTARE ÎN FAŢA INSTANŢELOR DE JUDECATĂ ȘI INFORMARE PUBLICĂ

## Secțiunea 1
## Avizarea actelor normative

În anul 2025, Autoritatea națională de supraveghere a emis, în conformitate cu atribuțiile stabilite prin prevederile art. 57 alin. (1) lit. c) din Regulamentul (UE) 2016/679, **avize** asupra unui număr de **84 de proiecte de acte normative** transmise de instituții publice, care implicau aspecte diferite privind prelucrarea datelor cu caracter personal.




**Proiectele de acte normative au fost transmise de către anumite ministere, precum Ministerul Mediului, Apelor și Pădurilor, Ministerul Sănătății, Ministerul Afacerilor Interne, Ministerul Fondurilor Europene, Ministerul Muncii si Solidarității Sociale, Ministerul Mediului, Apelor ș Pădurilor, dar și de către alte autorități sau instituții publice centrale.**

În majoritatea cazurilor, Autoritatea națională de supraveghere a efectuat o serie de observații și propuneri, prin raportare la necesitatea armonizării unor dispoziții din proiectele respective cu principiile și condițiile de prelucrare a datelor cu caracter personal.

În continuare, **prezentăm câteva dintre cele mai importante proiecte de acte normative transmise în vederea avizării:**

- **Ministerul Mediului, Apelor și Pădurilor a transmis proiectul de Ordonanță pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 17/2005 pentru stabilirea unor măsuri organizatorice la nivelul administrației publice centrale**

Faţă de conținutul proiectului de act normativ supus atenţiei, Autoritatea naţională de supraveghere a subliniat, raportat la prevederile art. $2^1$ din Ordonanța pentru modificarea și completarea O.U.G. nr. 17/2005, necesitatea clarificării și completării textului cu prevederi referitoare la:

- interzicerea prelucrării datelor personale în alte scopuri, raportat la prevederile art. 6 alin. (4) din Regulamentul (UE) 2016/679;
- identificarea categoriilor de persoane a căror imagine va fi prelucrată;
- stabilirea perioadei de stocare a datelor;
- stabilirea operațiunilor de ștergere ori distrugere după expirarea perioadei de stocare.

Sub acest aspect, Autoritatea naţională de supraveghere a recomandat să fie avute în vedere și prevederile art. 56 din Legea nr. 218/2002, republicată, privind organizarea și funcționarea Poliției Române.

Faţă de textul proiectului sus-menționat, Autoritatea naţională de supraveghere a propus și introducerea unui nou articol în textul de Ordonanță referitor la faptul că Garda Națională de Mediu prelucrează date cu caracter personal cu respectarea Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi

privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), precum și a celorlalte acte normative aplicabile domeniului protecției datelor personale.

Ministerul Mediului, Apelor și Pădurilor a retransmis Autorităţii naţionale de supraveghere proiectul de act normativ, însă fără a aduce modificări în sensul celor solicitate de instituția noastră.

Față de textul proiectului și având în vedere că nu au fost luate în considerare propunerile instituției noastre, Autoritatea națională de supraveghere a menținut observațiile formulate anterior și a avizat cu observații acest proiect.

- **Consiliului Concurenței a supus avizării Autorității naționale de supraveghere proiectul de Ordonanță de urgență a Guvernului pentru modificarea și completarea unor acte normative.**

Față de textul propunerii de act normativ supus atenției Autorității naționale de supraveghere, s-a subliniat că, raportat la art. 53 din Constituția României și la jurisprudența constantă a Curții Constituționale a României (Decizia nr. 458/2020 - considerentul 59), prin instrumentul de adoptare propus (Ordonanța de urgență) nu se poate restrânge dreptul la protecția datelor și viață privată, consacrat de art. 26 din Constituția României, de art. 7 și art. 8 din Convenția Europeană a Drepturilor Omului (CEDO), precum și de art. 16 din Tratatul privind Funcționarea Uniunii Europene (TFUE).

Referitor la art. I pct. 11 din proiectul de ordonanță de urgență privind prevederile art. 34 alin. (12) și (13) din Legea nr. 21/1996 a concurenței, prin care se instituie limitări ale drepturilor persoanelor fizice, s-a subliniat că este necesară completarea acestuia prin raportare la dispozițiile art. 23 alin. (2) din Regulamentul (UE) 2016/679, potrivit cărora orice măsură legislativă menţionată la alin. (1) al aceluiași articol trebuie să conțină cel puțin dispoziţiile specifice din alin. (2) al aceluiași articol.

În același timp, raportat la art. I pct. 11 din proiectul de ordonanță de urgență referitor la art. 34 alin. (13) din Legea nr. 21/1996, s-a precizat că drepturile persoanelor vizate nu pot fi restricționate/restrânse decât prin dreptul uniunii sau dreptul intern (nu prin regulament al Consiliului Concurenței) și numai "în măsura în care acest lucru este necesar şi proporţional într-o societate democratică pentru a se garanta siguranţa publică, inclusiv

protecţia vieţii oamenilor, în special ca răspuns la dezastre naturale sau provocate de om, prevenirea, investigarea şi urmărirea penală a infracţiunilor sau executarea pedepselor, inclusiv protejarea împotriva ameninţărilor la adresa siguranţei publice sau împotriva încălcării eticii în cazul profesiilor reglementate şi prevenirea acestora, alte obiective importante de interes public general ale Uniunii sau ale unui stat membru, în special un interes economic sau financiar important al Uniunii sau al unui stat membru, menținerea de registre publice din motive de interes public general, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a transmite informaţii specifice legate de comportamentul politic în perioada regimurilor fostelor state totalitare, protecţia persoanei vizate sau a drepturilor şi libertăţilor unor terți, inclusiv protecţia socială, sănătatea publică şi scopurile umanitare. Aceste restricții ar trebui să fie conforme cu cerinţele prevăzute de cartă şi de Convenția europeană pentru apărarea drepturilor omului şi a libertăţilor fundamentale", conform considerentului 73 din Regulamentul (UE) 2016/679.

Totodată, s-a subliniat că art. I pct. 11 din proiect nu conține garanțiile prevăzute la art. 23 alin. (2) din Regulamentul (UE) 2016/679.

Referitor la "furnizarea în masă și gratuit" a datelor reprezentanților legali ai întreprinderilor din economia națională fără a fi prevăzute garanții adecvate de către operatorii de date personale, de drept public, prevăzută la art. I pct. 11 din proiect privind art. 34 alin. (14) din Legea nr. 21/1996, Curtea Constituțională a României subliniază în Decizia nr. 461/2014 că "(...) ingerinţa în drepturile fundamentale privind viaţa intimă, familială şi privată, secretul corespondenței şi libertatea de exprimare este de o mare amploare şi trebuie considerată ca fiind deosebit de gravă, iar împrejurarea că păstrarea datelor şi utilizarea lor ulterioară sunt efectuate fără ca abonatul sau utilizatorul înregistrat să fie informat cu privire la aceasta este susceptibilă să imprime în conștiința persoanelor vizate sentimentul că viaţa lor privată face obiectul unei supravegheri constante."

În concluzie, în decizia mai sus amintită, Curtea Constituțională a României constată că legea supusă controlului de constituționalitate "nu respectă condiţiile impuse de principiul proporționalității, nu oferă garanţii care să asigure confidenţialitatea datelor cu caracter personal, aducând atingere însăși esenței drepturilor fundamentale referitoare la viaţă intimă, familială şi privată.

Autoritatea națională de supraveghere a solicitat reanalizarea și modificarea proiectului de act normativ.

- **Institutul Național de Statistică (I.N.S.) a supus avizării Autorității naționale de supraveghere proiectul de Lege privind registrul statistic de populație.**

Ca observație cu caracter general, Autoritatea națională de supraveghere a subliniat faptul că înființarea și organizarea registrului statistic de populație (RESPOP), în vederea elaborării statisticilor oficiale de populație de către I.N.S., presupune efectuarea de prelucrări masive de date cu caracter personal (inclusiv date sensibile) care ar trebui să respecte condițiile de legalitate și principiile prevăzute, în principal, de Regulamentul (UE) 2016/679.

Astfel, în ceea ce privește semnificația unor termeni și expresii generale de la art. 2 din proiectul de lege (de ex. "înregistrări individuale", "procesarea datelor în scop statistic", "scop statistic"), s-a propus reanalizarea acestora cu respectarea criteriilor de claritate, precizie, previzibilitate şi predictibilitate pe care un text de lege trebuie să le îndeplinească raportat la Decizia Curții Constituționale a României nr. 26/2012 și la prevederile Legii nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative.

În același timp, s-a precizat că în nota de fundamentare nu se regăsește o prevedere legală expresă care ar permite transmiterea către I.N.S. a extrem de multe date personale (inclusiv sensibile) deținute de atât de multe instituții publice din România, raportat la prevederile art. 6 și art. 9 din Regulamentul (UE) 2016/679.

De asemenea, nici în conținutul proiectului de act normativ nu a fost identificat temeiul legal în baza căruia I.N.S. ar fi abilitat să obțină date personale de la autoritățile publice menționate la art. 5 din proiect.

S-a subliniat că instituțiile publice mai sus menționate (cu activitate diferită și scopuri distincte) dețin sisteme de evidență în alte scopuri prevăzute de lege decât scopul de constituire a registrului statistic de populație prevăzut pentru I.N.S. de proiectul de lege, sens în care este necesar să fie respectate prevederile art. 6 alin. (4) din Regulamentul (UE) 2016/679 care instituie exigența compatibilității între scopul inițial al prelucrării și cel ulterior și care trebuie să se reflecte în dreptul intern aplicabil operatorului, pentru a se institui garanții adecvate protejării drepturilor persoanelor vizate.

Totodată, s-a propus reformularea mențiunilor de la Secțiunea a 2-a punctul 2.3. din expunerea de motive și a celor de la art. 9 din proiectul de lege referitoare la cadrul legislativ din domeniul protecției datelor, astfel: „Prelucrarea datelor cu caracter personal efectuată de I.N.S. în aplicarea prezentei legi se realizează cu respectarea prevederilor Regulamentului (UE) 679/2016 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), precum și a legislației naționale aplicabile domeniului protecției datelor."

În același timp, s-a subliniat că în conținutul proiectului de act normativ nu au fost identificate garanțiile prevăzute de art. 6 alin. (3) și nici cele instituite de art. 89 din Regulamentul (UE) 2016/679, fiind astfel necesară reanalizarea și completarea proiectului sub acest aspect.

De asemenea, s-a precizat că la proiectul de act normativ nu a fost atașată dovada realizării unei evaluări de impact în conformitate cu prevederile art. 35 alin. (10) din Regulamentul (UE) 2016/679 raportat la prelucrarea masivă de date (inclusiv date sensibile).

Astfel, prin raportare la dispozițiile alin. (10) al art. 35 din Regulamentul (UE) 2016/679, s-a apreciat că este necesară realizarea unei evaluări de impact la emiterea actului normativ, întrucât prelucrările de date preconizate a fi legiferate prin această propunere sunt realizate pe scară largă și în lipsa unor garanții, ceea ce poate aduce atingere dreptului la protecția datelor și viața privată a unui număr foarte mare persoane fizice.

Prin urmare, raportat la prelucrările masive de date personale preconizate (datele deținute de numeroase instituții publice din România), s-au subliniat aspectele statuate de Curtea Constituțională a României prin Decizia nr. 461/2014, potrivit cărora un act normativ trebuie să respecte principiul proporționalității, să ofere garanții care să asigure confidențialitatea datelor cu caracter personal, astfel încât să nu se aducă atingere drepturilor fundamentale referitoare la viața intimă, familială și privată, precum și libertății de exprimare.

Autoritatea națională de supraveghere a solicitat reanalizarea și modificarea proiectului de act normativ referitor la Legea privind registrul statistic de populație.

- **Ministerul Sănătății a supus avizării Autorității naționale de supraveghere proiectul de Ordonanță a Guvernului pentru modificarea Legii nr. 95/2006 privind reforma în domeniul sănătăţii şi pentru modificarea şi completarea unor acte normative în domeniul sănătăţii.**

Proiectul de act normativ nu a fost transmis în prealabil Autorității naționale de supraveghere în vederea formulării de observații și propuneri, potrivit dispozițiilor Hotărârii Guvernului nr. 561/2009 pentru aprobarea Regulamentului privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea şi prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum şi a altor documente, în vederea adoptării/aprobării.

Însă, având în vedere conţinutul proiectului de act normativ supus atenției Autorității naționale de supraveghere, raportat la dispozițiile Regulamentului (UE) 2016/679, au fost formulate următoarele observații și propuneri:

• Cu privire la Art. I pct. 1 din proiect prin care se care modifică art. $6^2$ din Legea nr. 95/2006 privind reforma in domeniul sănătăţii, republicată, cu modificările și completările ulterioare, s-a precizat că este necesară reanalizarea și completarea acestuia, raportat la prelucrările de date preconizate a fi efectuate în Registrul unic de evidență al unităților sanitare (RUEUS) și la noțiunea de operator de date cu caracter personal, așa cum este acesta definit în art. 4 pct. 7 din Regulamentul (UE) 2016/679.

În acest sens, rezultă că în cuprinsul art. $6^2$ trebuie precizat faptul că Ministerul Sănătății are calitate de operator de date cu caracter personal și urmează să gestioneze Registrul unic de evidență al unităților sanitare (RUEUS).

De asemenea, s-a subliniat că este necesară modificarea alin. (4) al art. $6^2$ din proiect în sensul înlocuirii cuvântului "înregistrarea" cu "prelucrarea".

Totodată, s-a menționat că este necesară modificarea alin. (5) al art. $6^2$ din proiect și reanalizarea sintagmei "operatori ai aplicației RUEUS", întrucât "persoanele cu atribuţii stabilite de conducerea Ministerului Sănătăţii şi a direcţiilor de sănătate publică judeţene şi a municipiului Bucureşti", la care se face referire în acest alineat, nu sunt operatori de date în sensul definiției operatorului din art. 4 pct. 7 din Regulamentul (UE) 2016/679.

S-a subliniat, totodată, că potrivit art. 29 din Regulamentul (UE) 2016/679 "Persoana împuternicită de operator şi orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru."

Ca atare, persoanele menționate la alin. (5) al art. $6^2$ din proiect sunt persoane care au acces, respectiv prelucrează date în RUEUS (de regulă, în calitate de angajați) și care acționează sub autoritatea operatorului sau a unei persoane împuternicite de operator.

• Referitor la Art. II din proiect prin care se modifică Art. V din OUG nr. 180/2020, s-au formulat următoarele:

a) Pentru claritatea textului este necesară reanalizarea formulării textului alin. (1) a art. V din proiect;

b) În același timp, cu privire la alin. (1) a art. V din proiect, se impune reanalizarea pe fond a prevederii, în sensul clarificării normei care se referă la preluarea tuturor datelor înregistrate în aplicația informatică "Corona-forms", în noua aplicație informatică ce ar urma să fie dezvoltată de Serviciul de Telecomunicații Speciale pentru Institutul Național de Sănătate Publică în vederea raportării bolilor transmisibile.

S-a precizat că art. 5 alin. (1) lit. b) din Regulamentul (UE) 2016/679 prevede că datele cu caracter personal trebuie să fie "colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri (...)" .

Astfel, având în vedere ca scopul declarat al noii aplicații este cel de raportare a bolilor transmisibile, rezultă că preluarea tuturor datelor înregistrate în aplicația informatică "Corona-forms" și prelucrarea acestora pe o perioadă nedeterminată (așa cum se prevede la alin. 4 al art. V din proiect), într-un alt scop decât cel pentru care au fost colectate inițial (combaterea efectelor generate de coronavirusul SARS-CoV-2), pune problema compatibilității cu principiile de prelucrare statuate de art. 5 din Regulamentul (UE) 2016/679.

Mai mult, Autoritatea națională de supraveghere a subliniat faptul că este necesară reanalizarea prevederilor alin. (1) a art. V din proiect și prin raportare la principiul necesității, prevăzut de art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679, care prevede că datele colectate trebuie să fie "adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate" .

c) Se impune necesitatea identificării și denumirii aplicației informatice dezvoltate pentru Institutul Național de Sănătate Publică în vederea raportării bolilor transmisibile;

d) Cu privire la alin. 4 al art. V din proiect, este necesară reanalizarea prevederilor referitoare la termenul de păstrare a datelor, respectiv "pe toată perioada de viață a persoanei vizate", raportat la necesitatea păstrării de date medicale (inclusiv date asociate cu afecțiuni medicale, altele decât cele referitoare la boli transmisibile, așa cum sunt cele înregistrate deja în Corona-forms – de ex. istoric vaccinări) și la principiul limitării legate de stocare, prevăzut de art. 5 alin. (1) lit. e) din Regulamentul (UE) 2016/679, care prevede că datele sunt "păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele".

e) La art. V alin. (8) lit. c) din proiect este necesară reanalizarea și reformularea sintagmei "au calitatea de operatori ai aplicației", precum și eliminarea referirii la "structurile de specialitate din cadrul ministerelor şi instituțiilor cu rețea sanitară proprie" ca fiind operatori ai aplicației, raportat la prevederile art. 4 pct. 7 (definiția operatorului de date cu caracter personal) și art. 29 din Regulamentul (UE) 2016/679.

În acest context, raportat la prevederile alin. (2), (6), (7) și (8) din art. V din proiect s-a considerat că este necesară stabilirea clară a entității care are calitatea de operator de date cu caracter personal pentru prelucrările de date din aplicație creată în vederea raportării bolilor transmisibile.

Din proiect rezultă că Institutul Național de Sănătate Publică și Ministerul Sănătății ar avea calitatea de operatori de date cu caracter personal.

Față de toate cele de mai sus, în legătură cu prelucrările de date cu caracter personal efectuate în contextul creării, dezvoltării și administrării unor noi aplicații, raportat la condițiile de legitimitate și principiile prelucrării datelor cu caracter personal, rezultă necesitatea reanalizării și modificării substanțiale a proiectului supus atenției Autorității naționale de supraveghere, astfel încât să răspundă exigențelor legislației europene și naționale în domeniul protecției datelor.

Ca atare, a fost semnată cu observații, în original, Nota de fundamentare a proiectului sus menționat, însoțită de documentele anexate acestuia.

- **Ministerul Sănătății a supus avizării Autorității naționale de supraveghere proiectul de Hotărâre a Guvernului privind înființarea, organizarea și funcționarea Registrului național de screening pentru cancerul de col uterin, Registrului național de screening pentru cancerul colorectal și Registrului național de screening pentru cancerul de sân.**

Autoritatea națională de supraveghere a formulat o observație cu titlu general și a subliniat faptul că, potrivit art. 16 din Regulamentul privind procedurile, la nivelul Guvernului, pentru elaborarea, avizarea şi prezentarea proiectelor de documente de politici publice, a proiectelor de acte normative, precum şi a altor documente, în vederea adoptării/aprobării aprobat prin Hotărârea nr. 561/2009, cu modificările și completările ulterioare, proiectul de hotărâre nu a fost transmis în faza preliminară pentru a se obține un punct de vedere din partea instituției noastre.

Față de conținutul proiectului de hotărâre emis în temeiul art. $6^1$ din Legea nr. 95/2006 și supus direct avizării, s-a precizat că activităţile desfăşurate în legătură cu înființarea, organizarea și funcționarea Registrului național de screening pentru cancerul de col uterin, Registrului național de screening pentru cancerul colorectal și a Registrului național de screening pentru cancerul de sân, așa cum se regăsesc în proiectul transmis autorității, presupun efectuarea de operaţiuni de prelucrare de date personale, cu precădere date sensibile privind starea de sănătate, care trebuie să respecte principiile de prelucrare prevăzute în Regulamentul (UE) 2016/679.

Referitor la nivelul normativ prin care se realizează reglementarea proiectului de act normativ (hotărâre de Guvern), raportat la necesitatea unui nivel înalt de protecție a datelor cu caracter medical și la art. 53 din Constituția României, s-a subliniat faptul că, în jurisprudența sa (Decizia nr. 498/2018 asupra dispozițiilor din Legea nr. 95/2006 referitoare la Dosarul Electronic de Sănătate), Curtea Constituțională a statuat următoarele:

"42. Cu alte cuvinte, dacă statul a instituit, prin lege, o măsură în aplicarea dreptului la ocrotirea sănătății persoanei, tot acestuia îi revine obligația de a proteja şi garanta caracterul confidențial al informațiilor medicale prelucrate, printr-un act normativ de același nivel, respectiv prin lege. Astfel, din acest punct de vedere, obligaţiile pozitive asociate celor două drepturi sunt corelative şi interdependente, trebuind să existe un just echilibru între

acestea. Statului nu îi este permis ca, protejând un drept constituţional, să o facă în detrimentului celuilalt drept deopotrivă ocrotit, pentru că s-ar putea ajunge la situaţia în care afectarea acestuia din urmă să fie atât de puternică, încât avantajul iniţial obținut să apară ca fiind nesemnificativ în această ecuație. Prin urmare, la nivel normativ, complementaritatea şi proporționalitatea trebuie să caracterizeze relaţia dintre cele două drepturi constituționale antereferite.

52. Prin urmare, revine legiuitorului obligaţia de a reglementa garanţiile asociate dreptului la viaţă intimă, familială şi privată. Această obligaţie trebuie să se materializeze prin lege, în sens de instrumentum.

55. (...) Având în vedere această situație normativă şi caracterul direct aplicabil al regulamentului antereferit [Regulamentul general privind protecția datelor – subl. ns.], legiuitorul trebuie să asigure o protecţie specifică datelor medicale, prin stabilirea unor garanţii puternice, care să ateste nivelul înalt de protecţie a datelor cu caracter medical."

În acest context, Autoritatea națională de supraveghere a subliniat necesitatea asigurării unei aplicări adecvate, în special, a dispozițiilor art. 5, art. 6 și art. 9, coroborate cu art. 24 și art. 25 din Regulamentul (UE) 2016/679, în domeniul reglementat prin proiectul transmis.

Referitor la art. 3, art. 13 și art. 23 din proiect, s-a considerat că este necesară clarificarea calității de operator a Centrului Național de Supraveghere al Bolilor Netransmisibile și a Centrului Național de Statistică în Sănătate Publică întrucât din mențiunile efectuate rezultă că acestea ar avea calitatea de persoane împuternicite, în sensul art. 4 pct. 8 din Regulamentul (UE) 2016/679.

Astfel, în măsura în care pentru aceste entități se stabilește calitatea de împuternicit, este necesar a se avea în vedere și dispozițiile art. 28 din Regulamentul (UE) 2016/679.

Cât privește art. 4, art. 14 și art. 24 din proiect, s-a precizat că în conținutul acestora nu sunt menționate datele cu caracter personal ori categoriile de date cu caracter personal care urmează a fi prelucrate în fișa unică și în Registrul național de screening pentru cancerul de col uterin, Registrul național de screening pentru cancerul colorectal și în Registrul național de screening pentru cancerul de sân.

În acest sens s-a pronunțat Curtea Constituțională a României, prin Decizia nr. 498/2018, subliniind următoarele:

"37. În cauza de față, Curtea constată că instituirea dosarului electronic de sănătate s-a realizat prin lege, fără ca aceasta să prevadă datele pe care dosarul urmează a le cuprinde. (...) În consecință, întrucât legea nu prevede obiectul dosarului electronic de sănătate, numai din coroborarea textului legal cu cel al normelor metodologice, în interpretarea normei, se poate ajunge la concluzia că dosarul electronic de sănătate cuprinde date personale de natură medicală.

46. Faptul că legea indică titularii dreptului de a asigura condițiile de mobilitate a informației medicale în format electronic nu poate fi văzut decât ca o măsură strict organizatorică, textul legii neindicând cine, în ce moment și ce date introduce în dosarul electronic de sănătate; (...) Mai mult, nu reiese scopul pentru care este introdusă și eventual folosită informația medicală. Astfel, Curtea constată că o măsură pozitivă a statului, chiar bine intenționată, poate produce efecte negative de o amploare deosebită în privința vieții private a persoanei."

Referitor la aceleași aspecte, Autoritatea națională de supraveghere a subliniat că la stabilirea datelor, respectiv a categoriilor de date cu caracter personal care sunt prelucrate prin intermediul registrelor menționate mai sus, urmează a se avea în vedere respectarea principiilor legate de prelucrarea datelor, stabilite de art. 5 Regulamentul (UE) 2016/679 (legalitate, transparență, limitări legate de scop, reducerea la minimum a datelor, exactitate, integritate și confidențialitate).

Autoritatea națională de supraveghere a menționat că este necesară identificarea și menționarea în proiectul de hotărâre a tuturor datelor/categoriilor de date cu caracter personal care urmează a fi prelucrate (în sensul definiției din art. 4 pct. 1 din Regulamentul (UE) 2016/679) cu respectarea "principiului reducerii la minimum a datelor" prevăzut în art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679 și cu instituirea garanțiilor prevăzute de art. 6 alin. (3) din același act normativ european.

În acest sens, s-au subliniat aspectele statuate de Curtea Constituțională a României prin Decizia nr. 461/2014, potrivit cărora un act normativ trebuie să respecte principiul proporționalității, să ofere garanții care să asigure confidențialitatea datelor cu caracter personal, astfel încât să nu se aducă atingere drepturilor fundamentale referitoare la viața intimă, familială și privată, precum și libertății de exprimare.

De asemenea, s-a considerat că sintagma "surse multiple" din cuprinsul art. 1, art. 2, art. 11, art. 12, art. 21 și art. 22 din proiectul de hotărâre este neclară și de natură să

producă confuzie cu privire la modalitatea de obținere a datelor, sens în care considerăm necesară reformularea acesteia și precizarea exactă a surselor publice/private avute în vedere.

Față de aceste aspecte, s-a menționat că este necesar a se avea în vedere și prevederile art. 6 alin. (4) din Regulamentul (UE) 2016/679 care instituie exigența compatibilității între scopul inițial al prelucrării și cel ulterior, care trebuie să se reflecte în dreptul intern aplicabil operatorului, pentru a se institui garanții adecvate protejării drepturilor persoanelor vizate.

În ceea ce privește dispozițiile art. 7 alin. (1), art. 17 alin. (1) și art. 27 alin. (1) din proiect, s-a precizat că se impune completarea acestora în sensul că dezvoltarea și operaționalizarea aplicației informatice de înregistrare nominală a datelor femeilor care au beneficiat de servicii medicale de screening pentru cancerul de col uterin, a persoanelor care au beneficiat de servicii medicale de screening pentru cancerul colorectal și a femeilor care au beneficiat de servicii medicale de screening pentru cancerul de sân, se realizează în concordanță cu principiile stabilite de Regulamentul (UE) 2016/679, inclusiv a principiilor privacy by design și by default prevăzute la art. 25 din Regulament și cel al proporționalității statuat de art. 5 din Regulamentul (UE) 2016/679.

De asemenea, pentru claritatea textului, față de conținutul art. 8 alin. (3), art. 18 alin. (3) și art. 28 alin. (3) din proiect, în ceea ce privește respectarea confidențialității datelor și aplicarea măsurilor de protecție a acestora, s-a subliniat faptul că Institutul Național de Sănătate Publică, în calitate de operator, are obligația de a implementa măsuri tehnice și organizatorice adecvate pentru a garanta protecția datelor cu caracter personal, în conformitate cu dispozițiile art. 32 din Regulamentului (UE) 2016/679, iar nu persoanele care au acces la SEESCCU, SEESROC și SEESCS (cum este menționat în proiect).

Autoritatea națională de supraveghere a propus reformularea prevederilor de la art. 8 alin. (4), art. 18 alin. (4) și art. 28 alin. (4) din proiectul de act normativ referitoare la cadrul legislativ din domeniul protecției datelor, în sensul că entitățile implicate în efectuarea de prelucrări de date în legătură cu SEESCCU, SEESROC și SEESCS au obligația respectării dispozițiilor Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei

95/46/CE (Regulamentul general privind protecția datelor), precum și a legislației naționale aplicabile domeniului protecției datelor.

În același timp, s-a considerat că prevederile art. 8 alin. (6) art. 18 alin. (6) și art. 28 alin. (6) din proiect, sunt contradictorii în ceea ce privește perioada de stocare a datelor. Astfel, pe de o parte se menționează că datele sunt stocate pe durata de viață a persoanei, iar pe de altă parte, în teza a doua, se precizează că ulterior perioadei necesare îndeplinirii scopului în care au fost prelucrate, datele vor fi șterse.

Astfel, s-a precizat că este necesară clarificarea acestor aspecte și stabilirea unui termen de stocare raportat la principiul prevăzut de art. 5 alin. (1) lit. e) din Regulamentul (UE) 2016/679 potrivit căruia datele trebuie păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele (principiul limitării legate de stocare), precum și stabilirea clară a ștergerii/distrugerii datelor ulterior și a responsabilității entităților implicate.

Prin urmare, având în vedere natura sensibilă a datelor personale privind starea de sănătate, s-a menționat că acestea nu pot fi prelucrate decât în măsura în care prelucrările de date stabilite prin dreptul intern se subsumează exigențelor legislației europene și naționale în domeniul protecției datelor, precum și jurisprudenței Curții Constituționale a României.

Autoritatea națională de supraveghere a subliniat, în acest context, faptul că este necesară stabilirea unor garanții la nivel de lege care să ateste nivelul adecvat de protecție a datelor cu caracter medical fără a se aduce atingere drepturilor la protecția datelor și viață privată, consacrate de art. 26 din Constituția României, de art. 7 și 8 din Convenția europeană a drepturilor omului (CEDO), precum și de art. 16 din Tratatul privind funcționarea Uniunii Europene (TFUE).

Ca atare, a rezultat necesitatea reanalizării și modificării proiectului de act normativ supus direct avizării Autorității naționale de supraveghere.

- **Secretariatul General al Guvernului a transmis propunerea legislativă pentru completarea Legii nr. 272 din 21 iunie 2004 privind reforma în protecţia şi promovarea drepturilor copilului, republicată în Monitorul Oficial nr. 159 din 5 martie 2014 și pentru completarea Legii nr. 292 din 20 decembrie 2010 privind asistența socială, publicată în Monitorul Oficial nr. 905 din 20 decembrie 2011.**

Având în vedere conținutul propunerii legislative supusă atenției Autorității naționale de supraveghere, prin raportare la dispozițiile Regulamentului (UE) 2016/679, au fost subliniate următoarele:

În ceea ce privește expunerea de motive a propunerii legislative analizate, s-a subliniat că aceasta nu conține nicio justificare a clară și concretă a necesității modificării și completării actelor normative la care se referă, se întemeiază pe referiri vagi, generale, nefundamentate și necorelate cu alte acte normative care conțin dispoziții speciale referitoare la protecția categoriilor de persoane menționate în proiect și care necesită o protecție suplimentară (de ex. minori, persoane vulnerabile, bolnavi, angajați).

În același timp, având în vedere prelucrările de date care se intenționează a fi efectuate în contextul propunerii de act normativ, este de menționat faptul că acestea presupun, printre altele, nu doar efectuarea prelucrărilor de date cu caracter personal preconizate a fi realizate prin mijloace de supraveghere video, ci și prelucrarea de date cu caracter special (de ex. date privind sănătatea) care sunt reglementate în mod expres prin Regulamentul (UE) 2016/679 și care se referă la anumite categorii de persoane vizate cărora Regulamentul le oferă o protecție suplimentară.

S-a subliniat faptul că Regulamentul (UE) 2016/679 creează un nivel suplimentar de protecție în cazul în care sunt prelucrate datele cu caracter personal ale persoanelor fizice vulnerabile, în special ale copiilor.

În considerentul (38) din Regulament se precizează "Copiii au nevoie de o protecţie specifică a datelor lor cu caracter personal, întrucât pot fi mai puţin conştienţi de riscurile, consecinţele, garanţiile în cauză şi drepturile lor în ceea ce priveşte prelucrarea datelor cu caracter personal. (...)"

În considerentul (58) se statuează că: "Principiul transparenţei prevede că orice informaţii care se adresează publicului sau persoanei vizate să fie concise, uşor accesibile şi uşor de înţeles şi să se utilizeze un limbaj simplu şi clar, precum şi vizualizare acolo unde este cazul. (...) Acest lucru este important în special în situaţii în care datorită multitudinii actorilor şi a complexităţii, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să știe şi să înțeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine şi în ce scop, (...). Întrucât copii necesită o protecţie specifică, orice informaţii şi orice comunicare, în cazul în care prelucrarea vizează un copil, ar trebui să fie exprimate într-un limbaj simplu şi clar, astfel încât copilul să îl poată înţelege cu ușurință.

De asemenea, în considerentul (75) se precizează: "Riscul pentru drepturile şi libertăţile persoanelor fizice, prezentând grade diferite de probabilitate de materializare şi de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: (...) sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal şi afectează un număr larg de persoane vizate."

Mai mult, prin propunerea legislativă se preconizează nu doar o supraveghere permanentă a minorilor din centre de plasament ori a persoanelor aflate în situații de risc social beneficiare de servicii publice sau private de asistență socială, ci și o supraveghere video permanentă a angajaților acestor facilități.

Referitor la prelucrarea datelor angajaților la locul de muncă, s-a precizat că sunt aplicabile dispozițiile art. 88 din Regulamentul (UE) 2016/679 intitulat "Prelucrarea în contextul ocupării unui loc de muncă", precum și dispozițiile art. 5 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

Corelat cu cele de mai sus, potrivit art. 6 alin. (2) din Regulamentul (UE) 2016/679, statele membre pot menține sau introduce dispoziții mai specifice de adaptare a aplicării normelor regulamentului în ceea ce privește prelucrarea în vederea respectării unei obligații legale, prin definirea unor cerințe specifice mai precise cu privire la prelucrare şi a altor măsuri de asigurare a unei prelucrări legale şi echitabile, inclusiv pentru alte situații concrete

de prelucrare, astfel cum este prevăzut în capitolul IX al regulamentului (care conține și art. 88 mai sus citat).

În plus, s-a subliniat că, în cazul unui tip de prelucrare precum cea preconizată de propunerea de act normativ supusă analizei, care este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, în cadrul procesului de pregătire propunerii legislative era necesară realizarea unei evaluări a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal, în acord cu prevederile art. 36 alin. (4) din Regulamentul (UE) 2016/679.

Prin urmare, ca observație cu caracter general, s-a considerat că propunerea legislativă nu se subsumează exigențelor prevederilor Regulamentului (UE) 2016/679 și a prevederilor legale aplicabile în domeniul protecției datelor cu caracter personal, și nici nu instituie garanțiile prevăzute de regulament în ceea ce privește prelucrarea datelor cu caracter personal, precum și particularizarea acestora la situațiile specifice din proiect.

Astfel, propunerea legislativă nu conține în Art. I (care introduce art. $123^1$ în Legea nr. 272/2004) și în Art. II (care introduce art. $38^1$ în Legea nr. 292/2011) precizări specifice prelucrărilor de date cu caracter personal preconizate a fi efectuate prin mijloace de supraveghere video, printre care:

- Stabilirea calității entităților ("serviciile de tip rezidențial", respectiv "furnizorii de servicii sociale, publici sau privați") care ar urma să prelucreze date prin intermediul sistemelor de supraveghere video, raportat la prevederile art. 4 pct. 7 și 8 din Regulamentul (UE) 2016/679 (alin. 1 din art. $123^1$ din Legea nr. 272/2004, respectiv art. $38^1$ din Legea nr. 292/2011).

- Stabilirea scopurilor concrete în care sunt prelucrate datele, raportat la principiul stabilit de art. 5 alin. (1) lit. b) din Regulamentul (UE) 2016/679 prevede că datele cu caracter personal trebuie să fie "colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri (...)" .

Ca atare, se impune reanalizarea pe fond a prevederii din alin. 3 din art. $123^1$ din Legea nr. 272/2004, respectiv art. $38^1$ din Legea nr. 292/2011 în sensul clarificării normei care se referă la prelucrarea în scopul "monitorizării calităţii activităţii, investigării unor incidente sau pentru asigurarea securităţii persoanelor/beneficiarilor serviciilor sociale."

În contextul celor de mai sus, având în vedere scopurile declarate ale prelucrărilor din propunerea analizată, rezultă că este necesar să fie luate în considerare și prevederile art. 6

alin. (4) din Regulamentul (UE) 2016/679 care instituie exigența compatibilității între scopul inițial al prelucrării (de ex. "monitorizarea calității activității") și un scop ulterior (de ex. "investigarea unor incidente") și care trebuie să se reflecte în dreptul intern aplicabil operatorului, pentru a se institui garanții adecvate protejării drepturilor persoanelor vizate.

Mai mult, s-a subliniat că este necesară reanalizarea prevederilor menționate, prin raportare atât la principiul necesității, prevăzut de art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679, care prevede că datele colectate trebuie să fie "adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate", cât și la principiul limitării legate de stocare, prevăzut de art. 5 alin. (1) lit. e) din Regulamentul (UE) 2016/679, care prevede că datele sunt "păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele", raportat la perioada de stocare a datelor din înregistrările video ("minimum 30 de zile şi maximum 6 luni") specificată în propunerea analizată.

- Reglementarea modalității prin care se realizează informarea completă și corectă a tuturor persoanelor vizate (nu doar a persoanelor interesate), raportat la prevederile art. 13 din Regulamentul (UE) 2016/679 (alin. 4 din art. $123^1$ din Legea nr. 272/2004, respectiv art. $38^1$ din Legea nr. 292/2011).

- Reglementarea expresă în actele normative ale căror modificare/completare se intenționează prin propunerea de act normativ a garanțiilor necesare pentru protejarea drepturilor persoanelor vizate (de ex. modalitatea de exercitarea drepturilor prevăzute de regulament).

- Adoptarea unor măsuri tehnice și organizatorice concrete pe care "serviciile de tip rezidențial", respectiv "furnizorii de servicii sociale, publici sau privați" trebuie să le implementeze în vederea asigurării securității și confidențialității datelor cu caracter personal, raportat la principiile "integrității și confidențialității", respectiv "responsabilității„ din art. 5 alin. (1) lit. f și art. 5 alin. (2), coroborate cu prevederile art. 24 și art. 32 din Regulamentul (UE) 2016/679.

- Clarificarea aspectelor de fond legate de cuantumul și aplicarea sancțiunilor stabilite prin alin. (5) al art. $123^1$ din Legea nr. 272/2004 și art. $38^1$ din Legea nr. 292/2011, pentru nerespectarea noilor prevederi introduse din propunerea de act normativ (raportat de ex. la lipsa mențiunilor cu privire la organul constatator al noilor contravenții stabilite prin propunerea de act normativ).

S-a subliniat că la stabilirea acestor aspecte este necesar a se avea în vedere faptul că atribuții de control și sancționare a contravențiilor în domeniul protecției datelor cu caracter personal revin Autorității naționale de supraveghere, iar regimul sancționator este deja reglementat prin Regulamentul (UE) 2016/679 și Legea nr. 190/2018.

În plus, în contextul tuturor celor de mai sus, s-a subliniat că nu este suficientă utilizarea sintagmei "fără a compromite integritatea beneficiarilor de servicii sociale", respectiv trimiterea la conformitatea cu "normele legale privind protecția datelor cu caracter personal și drepturile acestora" din alin. (2) al art. $123^1$ din Legea nr. 272/2004 și art. $38^1$ din Legea nr. 292/2011, în contextul în care propunerea legislativ se referă la o monitorizare video continuă a mai multor categorii de persoane vizate, printre care și minori.

Astfel, s-a menționat că pentru prelucrările preconizate este necesară stabilirea și includerea în proiectul de act normativ a unor garanţii adecvate care să asigure respectarea drepturilor persoanelor vizate și a vieții private a acestora, sens în care s-a pronunțat și Curtea Constituțională a României în Decizia nr. 498/17 iulie 2018 (cu precădere considerentele 37, 45, 46, 49 și 50).

Autoritatea națională de supraveghere nu a susținut această propunere legislativă în forma prezentată și a recomandat reanalizarea acesteia sub aspectul observațiilor formulate anterior.

- **Secretariatul General al Guvernului a transmis Autorității naționale de supraveghere propunerea legislativă privind dreptul la petiționare și reglementarea soluționării petițiilor.**

Față de prevederile Regulamentului (UE) 2016/679, au fost formulate următoarele observații și propuneri:

În ceea ce privește expunerea de motive a propunerii legislative analizate, s-a apreciat că aceasta nu conține nicio justificare clară și concretă a necesității reglementării unei activități deja reglementate prin Ordonanța nr. 27/2002 privind reglementarea activității de soluționare a petițiilor, cu modificările și completările ulterioare, se întemeiază pe referiri generale, nefundamentate și necorelate cu alte acte normative care conțin dispoziții speciale legate de activitatea de soluționare a petițiilor.

Referitor la îndeplinirea obligațiilor instituite în sarcina autorităților/instituțiilor publice, inclusiv prin utilizarea unui nou registru electronic (Registrul electronic al petițiilor - REP), comun sau găzduit centralizat în cloud-ul guvernamental, s-a precizat că este necesară stabilirea unor standarde, reguli, obligații necesare activităților operaționale, procedurale și tehnice de organizare și funcționare a acestuia, astfel încât prelucrările masive de date cu caracter personal care se vor efectua în cadrul acestui nou sistem de evidență electronic să respecte prevederile exprese din Regulamentul (UE) 2016/679, din Legea nr. 190/2018 și din celelalte acte normative aplicabile domeniului protecției datelor.

Ca atare, analizând propunerea legislativă supusă atenției Autorității naționale de supraveghere, s-au subliniat următoarele:

Este necesară reanalizarea și reformularea prevederilor art. 10 alin. (6) din propunere, având în vedere faptul că alineatul face referire la respectarea dispozițiilor Regulamentului (UE) 2016/679, deși conținutul alineatului face referire la metatdate, noțiune distinctă de cea de date cu caracter personal definită în art. 4 pct. 1 din același act normativ.

Referitor la prevederile art. 10 alin. (7) din propunere este necesară stabilirea calității de operator, respectiv împuternicit a "UAT cu micro-structură administrativă" care vor "externaliza păstrarea metadatelor şi a jurnalelor tehnice" și a "furnizorului platformei REP partajate", raportat la prevederile art. 4 pct. 7 și 8 din Regulamentul (UE) 2016/679.

Cu privire la prevederile din art. 16 și art. 17 din propunere s-a remarcat faptul că în registrul electronic al petițiilor (REP) vor fi înregistrate atât date privind identitatea petiționarilor, cât și solicitările scrise ale acestora, petițiile primite telefonic, înregistrări audio ori fișiere audio, video, imagini legate de petiții, precum și răspunsurile comunicate (art. 17 alin. (3) din propunere), iar la acest registru pot avea acces atât petiționarii cât și unitățile administrativ-teritoriale care pot utiliza un fie un REP "comun operat la nivel județean/asociație de dezvoltare intercomunitară" (art. 17 alin. (8) din propunere) fie pot conecta REP utilizat cu sisteme similare ale altor autorități (art. 17 alin. 12 din propunere), ceea ce presupune o serie de riscuri legate de prelucrarea datelor cu caracter personal.

S-a subliniat faptul că diseminarea în spațiul virtual a datelor persoanelor fizice identificate/identificabile (petiționarii, persoane vizate, potrivit Regulamentului (UE) 2016/679) și, implicit, punerea la dispoziția unui număr potențial foarte mare de persoane, fără control asupra utilizării ulterioare a datelor în scopuri posibil incompatibile cu scopul

inițial, poate reprezenta o ingerință gravă în drepturile la viaţă privată și protecția datelor cu caracter personal, astfel cum sunt garantate de art. 26 din Constituție, art. 8 din Convenția Europeană a Drepturilor Omului, precum și art. 7 și 8 din Carta Drepturilor Fundamentale a Uniunii Europene.

În acest context, s-a subliniat faptul că și în situația în care printre informațiile publicate în REP nu figurează numele sau adresa unui petiționar, este posibil să se recunoască persoana respectivă pe baza criteriilor socio-economice, culturale sau a altor criterii sau informații din petițiile depuse. Cu alte cuvinte, posibilitatea de a identifica o persoană, în contextul noilor tehnologii, nu mai înseamnă, în mod necesar, cunoașterea numelui și prenumelui și a adresei acesteia.

Raportat la cele de mai sus, față de publicarea în REP atât a solicitărilor petenților cât și a răspunsurilor aferente acestora (raportat și la prevederile art. 8 și art. 15 din Anexa nr. 1 la Lege - Norme metodologice de aplicare a Legii privind dreptul la petiționare şi reglementarea soluţionării petiţiilor) s-a subliniat faptul că în cuprinsul acestor documente pot exista o multitudine de informaţii și date cu caracter personal care pot conduce ulterior la (re)identificarea unei persoane fizice, prin combinarea cu alte informaţii existente în mediul on-line, ceea ce poate determina riscul apariției unor situaţii (posibil grave) de încălcare a drepturilor persoanelor fizice.

În plus, este de subliniat faptul că art. 25 din Regulamentul (UE) 2016/679 stabilește asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit, respectiv asigurarea principiilor privacy by design și by default.

Este de menționat faptul că în jurisprudența sa, Curtea de Justiție a Uniunii Europene a statuat faptul că "înainte de a divulga informații referitoare la o persoană fizică, instituțiile sunt ținute să pună în balanță interesul Uniunii de a garanta transparența acțiunilor sale și atingerea adusă drepturilor recunoscute prin articolele 7 și 8 din Cartă. Or, nu se poate recunoaște obiectivului transparenței nicio superioritate automată asupra dreptului la protecția datelor cu caracter personal (a se vedea în acest sens Hotărârea Comisia/Bavarian Lager, citată anterior, punctele 75-79), chiar dacă sunt în joc interese economice importante (Cauza 92 și 93/ 09 pct. 85)

Legat de aspectele anterioare, s-a subliniat și faptul că Regulamentul (UE) 2016/679 stabilește atât obligativitatea asigurării securității și confidențialității datelor personale (conform art. 32), ci și principiul responsabilității operatorului (art. 5 alin. 2, coroborat cu

art. 24 din regulament) – în cazul de față toate entitățile, din diverse domenii de activitate, ce ar urma să aplice dispozițiile propunerii de act normativ.

În același timp, în ceea ce privește realizarea unei "evaluări de impact asupra protecție datelor", s-a precizat că propunerea legislativă conține prevederi contradictorii. Astfel, pe de o parte se prevede că o astfel de evaluare ar fi obligatorie pentru entitățile care utilizează REP (de ex. art. 16 alin. (2) din propunere) și, pe de altă parte, se prevede că aceleași entități realizează "atunci când este necesar, o evaluare de impact asupra protecţiei datelor (DPIA)".

În ceea ce privește evaluarea impactului asupra protecţiei datelor, s-a subliniat că aceasta se realizează de către operatorii de date cu caracter personal potrivit art. 35 din Regulamentul (UE) 2016/679, cu luarea în considerare a dispozițiilor Deciziei nr. 174/2018 privind lista operaţiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecţiei datelor cu caracter personal, raportat la natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice.

Referitor la prevederile art. 18 alin. (9) din propunere, s-a considerat că este necesară reanalizarea acestora având în vedere faptul că încălcările securităţii datelor cu caracter personal sunt notificate ANSPDCP, potrivit art. 33 din Regulamentul (UE) 2016/679, iar notificarea este obligatorie și nu opțională ("după caz", cum se menționează în textul din propunere). Pe de lată parte, art. 34 din același regulament se referă la informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal.

Totodată, în ceea ce privește prevederile art. 18 alin. (10) din propunere, s-a subliniat că acestea trebuie reanalizate, în contextul în care nu doar încălcarea obligaţiilor prevăzute în acest articol atrage răspunderea potrivit legislaţiei privind protecţia datelor.

S-a mai subliniat că regimul sancționator la încălcărilor în materia datelor cu caracter personal sunt reglementate în principal în Regulamentul (UE) 2016/679 și, după caz, de Legea nr. 190/2018, pentru autorităţi şi organisme publice.

Cu privire la răspunderea disciplinară reglementată în art. 20 din propunerea legislativă, s-a considerat că aceste prevederi vin în contradicție cu atât cu dispozițiile cu caracter general din Capitolul II Răspunderea Disciplinară (art. 247 și următoarele) din Legea nr. 53/2003 – Codul muncii, republicat, cu modificările și completările ulterioare, cât

și cu dispozițiile din Ordonanța de Urgență nr. 57/2019 privind Codul administrativ, cu modificările și completările ulterioare (art. 493 și următoarele).

În ceea ce privește Anexa nr. 1 la Lege (Norme metodologice de aplicare a Legii privind dreptul la petiționare și reglementarea soluționării petițiilor) s-a subliniat că, în art. 18, sunt prevederi ce contravin reglementărilor stabilite de legiuitorul european în Regulamentul (UE) 2016/679 (de ex. cele privind încălcările de securitatea reglementate expres în art. 33 și 34 din Regulamentul (UE) 2016/679, cele referitoare la responsabilul cu protecția datelor desemnat la nivelul unui operator de date și ale cărui sarcini sunt cele prevăzute de art. 39, precum și cele privind evaluarea impactului asupra protecției datelor reglementate în art. 35 și 36 din același regulament).

Cu privire la cea de-a doua solicitare, referitoare la aspecte legate de implicații financiare impuse de aplicarea propunerii legislative, aceasta nu se circumscrie atribuțiilor Autorității naționale de supraveghere.

Totodată, luând în considerare implicațiile în ceea ce privește respectarea dreptului la petiționare, consacrat în art. 51 din Constituția României, republicată, Autoritatea națională de supraveghere a apreciat ca fiind oportună consultarea instituției Avocatul Poporului, raportat la atribuțiile acesteia, stabilite în Legea nr. 35/1997 privind organizarea și funcționarea instituției Avocatul Poporului, republicată.

Autoritatea națională de supraveghere nu a susținut această propunere legislativă.

## Secțiunea a 2-a:

## Puncte de vedere

În anul 2025 a fost adresat Autorității naționale de supraveghere un număr de **934 solicitări de emitere puncte de vedere** privind diverse aspecte referitoare la Regulamentul (UE) 2016/679, de către operatorii de date cu caracter personal și împuterniciții acestora, atât din domeniul public cât și din sectorul privat, precum și de către persoane fizice.

În acest an se poate remarca o ușoară creștere a numărului de solicitări față de anul anterior, însă menținerea unui nivel constant reliefează interesul operatorilor și al împuterniciților în asigurarea respectării regulilor de prelucrare a datelor personale instituite de Regulamentul (UE) 2016/679 și de legislația națională specifică, dar și cel al persoanelor vizate în ceea ce privește drepturile și condițiile de prelucrare a datelor cu caracter personal reglementate de actul normativ european.




**Prezentăm, în continuare, câteva dintre cazurile semnificative supuse atenției Autorității naționale de supraveghere, în vederea emiterii unor puncte de vedere, astfel:**

♦ ***Aplicarea Regulamentului (UE) 2016/679 în contextul derulării acțiunilor de monitorizare, evaluare, identificare, prevenire și combatere a segregării școlare în învățământul preuniversitar***

O persoană fizică a solicitat un punct de vedere referitor la conţinutul Ordinului nr. 7701/2024 privind aprobarea Metodologiei pentru monitorizarea, evaluarea, identificarea, prevenirea şi combaterea segregării şcolare în învăţământul preuniversitar.

Metodologia reglementează monitorizarea, identificarea, evaluarea și prevenirea segregării școlare, precum și intervenția în cazuri de segregare școlară și stabilește cadrul general pentru acțiunile de prevenire și monitorizare a segregării școlare, calendarul monitorizării, precum și acțiunile de prevenire a segregării școlare sau de intervenție în cazurile de segregare școlară din unitățile de învățământ preuniversitar.

În cadrul monitorizării și evaluării segregării școlare sau în cadrul acțiunilor de prevenire a segregării școlare, respectiv intervenție în cazuri de segregare școlară, unitățile de învățământ preuniversitar prelucrează o serie de date cu caracter personal, inclusiv categorii speciale de date personale ale elevilor minori sau majori care se află într-o astfel de situație.

Ca atare, față de conţinutul adresei, prin care petentul își exprima îngrijorarea în legătură cu prelucrările de date preconizate a fi efectuate în contextul aplicării Ordinului nr. 7701/2024, Autoritatea naţională de supraveghere a precizat următoarele:

În ceea ce privește legalitatea prelucrării datelor, Regulamentul (UE) 2016/679 stabilește că prelucrarea datelor cu caracter personal se realizează la consimțământul persoanei vizate sau în celelalte condiții prevăzute de art. 6, art. 9 și art. 10, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

În plus, s-a precizat că alin. (2) din Regulamentul (UE) 2016/679 prevede:

"(2) Statele membre pot menţine sau introduce dispoziţii mai specifice de adaptare a aplicării normelor prezentului regulament în ceea ce priveşte prelucrarea în vederea respectării alineatului (1) literele (c) şi (e) prin definirea unor cerinţe specifice mai precise cu privire la prelucrare şi a altor măsuri de asigurare a unei prelucrări legale şi echitabile, inclusiv pentru alte situaţii concrete de prelucrare, astfel cum este prevăzut în capitolul IX.

(3) Temeiul pentru prelucrarea menţionată la alineatul (1) literele (c) şi (e) trebuie să fie prevăzut în:

a) dreptul Uniunii; sau

b) dreptul intern care se aplică operatorului.

Scopul prelucrării este stabilit pe baza respectivului temei juridic sau, în ceea ce priveşte prelucrarea menţionată la alineatul (1) litera (e), este necesar pentru îndeplinirea

unei sarcini efectuate în interes public sau în cadrul exercitării unei funcţii publice atribuite operatorului. Respectivul temei juridic poate conţine dispoziţii specifice privind adaptarea aplicării normelor prezentului regulament, printre altele: condiţiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entităţile cărora le pot fi divulgate datele şi scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare;

şi operaţiunile şi procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale şi echitabile cum sunt cele pentru alte situaţii concrete de prelucrare astfel cum sunt prevăzute în capitolul IX. Dreptul Uniunii sau dreptul intern urmăreşte un obiectiv de interes public şi este proporţional cu obiectivul legitim urmărit."

Referitor la prelucrarea datelor privind originea rasială sau etnică, opiniile politice, confesiunea religioasă (religia) sau convingerile filozofice sau apartenența la sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea (date medicale) sau de date privind viaţa sexuală sau orientarea sexuală ale unei persoane fizice, s-a menționat că aceste prelucrări se supun prevederilor art. 9 din Regulamentul (UE) 2016/679.

Prin urmare, în contextul prelucrării datelor personale, este necesară analizarea temeiului legal al efectuării acesteia, în conformitate cu dispozițiile mai sus enumerate. În acest sens, în măsura în care nu există consimțământul persoanei vizate, datele personale ale acesteia pot fi prelucrate în celelalte situații menționate anterior, cum ar fi respectarea unei obligații legale, respectiv dacă prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul.

S-a menționat faptul că Regulamentul (UE) 2016/679 introduce, în art. 5, principiul responsabilității, potrivit căruia operatorii de date cu caracter personal nu numai că sunt responsabili de respectarea tuturor principiilor de prelucrarea a datelor, dar este necesar ca aceștia să poată demonstra respectarea principiilor menționate.

În ceea ce privește responsabilitatea operatorului, art. 24 din Regulamentul (UE) 2016/679 prevede că "Ținând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi

organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc şi se actualizează dacă este necesar."

În plus, operatorul și persoana împuternicită de acesta trebuie să asigure măsurile tehnice și organizatorice, în conformitate cu art. 32 și art. 24 din Regulamentul (UE) 2016/679.

În ceea ce privește Sistemul Informatic Integrat al Învățământului din România (SIIIR), Autoritatea națională de supraveghere a precizat următoarele:

Art. 5 alin. (2) din Regulament-cadru/2024 de organizare şi funcţionare a unităţilor de învăţământ preuniversitar, aprobat de Ordinul 5.726/2024, prevede:

"Unităţile de învăţământ care fac parte din reţeaua şcolară naţională au obligaţia de a include în Sistemul Informatic Integrat al Învăţământului din România (SIIIR), datele referitoare la beneficiarii primari şcolarizaţi."

Art. 68 din același Regulament-cadru prevede că profesorul diriginte are următoarele atribuția de a colabora cu "k) persoana desemnată pentru gestionarea SIIIR, în vederea completării şi actualizării datelor referitoare la elevi;" (persoana desemnată din cadrul unității de învățământ).

Același Regulament-cadru conține, în anexa 5, modelul Contractului educațional în care se prevăd drepturile dar și obligațiile părinților/reprezentanților legali ai beneficiarilor primari școlarizați (pct. IV), printre care:

"i) îşi exprimă acordul cu privire la prelucrarea datelor personale ale beneficiarului primar minor, conform cerinţelor Regulamentului UE nr. 679/2016;"

S-a menționat faptul că în art. 8 din Anexa Ordinului nr. 7701/2024 privind aprobarea Metodologiei pentru monitorizarea, evaluarea, identificarea, prevenirea şi combaterea segregării şcolare în învăţământul preuniversitar, se prevede:

"(1) În cadrul monitorizării și evaluării segregării școlare sau în cadrul acțiunilor de prevenire a segregării școlare, respectiv intervenție în cazuri de segregare școlară, unitățile de învățământ preuniversitar colectează, stochează și procesează date cu caracter personal. Scopul prelucrării acestor date este de a preveni segregarea școlară. Unitățile de învățământ preuniversitar, precum și toți factorii implicați au obligația să asigure protecția datelor cu caracter personal și confidențialitatea acestora în procesul de prelucrare pe care îl derulează.

(2) Părinții sau reprezentanții legali ai copiilor/elevilor raportează datele personale și contextuale ale copiilor lor, în conformitate cu prevederile Regulamentului-cadru de organizare și funcționare a unităților de învățământ preuniversitar și cu cele ale Contractului educațional. Datele personale și contextuale ale copiilor sunt utilizate strict pentru calcularea indicatorilor și scorurilor școlare reglementate prin prezenta metodologie și pentru implementarea politicilor Ministerului Educației pentru promovarea echității în educație. Pentru calcularea indicatorilor și scorurilor școlare reglementate prin prezenta metodologie pot fi utilizate și alte date stocate la nivelul unității școlare.

(3) Unitățile de învățământ preuniversitar au obligația de a colecta și raporta toate datele necesare calculării indicatorilor cuprinși în anexele prezentei metodologii."

Așadar, în ceea ce privește aspectele puse în discuție în adresa petentului referitoare la Ordinul nr. 7701/2024, Autoritatea națională de supraveghere a menționat că datele cu caracter personal ale elevilor din învățământul preuniversitar ce urmează a fi introduse în SIIIR - Sistemul Informatic Integrat al Învățământului din România, sunt prelucrate de operatorii de date cu caracter personal menționați anterior, respectiv unitatea de învățământ din domeniul învățământului preuniversitar și Ministerul Educației, întrucât prelucrarea este necesară în vederea îndeplinirii unei obligații legale ce le revine acestora.

Totodată, în contextul dat s-a subliniat faptul că este necesar ca un operator de date cu caracter personal precum cei menționați anterior să analizeze, în funcție de specificul tuturor activităților efectiv realizate, toate prelucrările de date personale efectuate, să stabilească temeiul acestora și să ia toate măsurile necesare pentru respectarea principiilor de prelucrare, a drepturilor persoanelor vizate, precum și pentru asigurarea securității și confidențialității datelor, raportat la prevederile legale din Regulamentul (UE) 2016/679 și din Legea nr. 190/2018, precum și din domeniul specific de activitate.

### ♦ *Aplicarea Regulamentului (UE) 2016/679 în contextul evaluării riscului de credit al persoanelor fizice*

O societate comercială cu răspundere limitată ce desfășoară activități de tip birou de credit pentru a evalua riscul de credit al persoanelor fizice care intenționează să acceseze credite de la instituții financiare bancare/non bancare (IFN) a solicitat un punct de vedere cu privire la posibilitatea stabilirii unui cadru de colaborare controlat și legal între aceasta și

alte instituții și entități publice (de ex. Direcția Generală Permise de Conducere și Înmatriculări, Agenția Națională de Cadastru și Publicitate Imobiliară, etc.).

Față de solicitarea respectivă, Autoritatea națională de supraveghere a precizat următoarele:

În ceea ce privește prelucrarea datelor cu caracter personal, Autoritatea națională de supraveghere a arătat că Regulamentul (UE) 2016/679 stabilește că prelucrarea datelor cu caracter personal, inclusiv sub aspectul dezvăluirii acestora, se realizează cu consimțământul persoanei vizate sau în celelalte situații, prevăzute de art. 6, art. 9 și art. 10 din regulament, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

Prin urmare, în contextul prelucrării (dezvăluirii) datelor personale, este necesară analizarea temeiului legal al efectuării acesteia, în conformitate cu dispozițiile Regulamentul (UE) 2016/679, anterior precizate. În acest sens, numai în măsura în care un operator identifică, de exemplu, faptul că prelucrarea este necesară pentru îndeplinirea unei obligații legale ori pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, datele pot fi prelucrate fără consimțământul persoanei vizate.

De asemenea, s-a precizat că Regulamentul (UE) 2016/679 stabilește, în art. 5, o serie de principii care se impun a fi respectate în cadrul prelucrării datelor (inclusiv al dezvăluirii).

S-a menționat că același articol prevede la alin. (2) că operatorul este responsabil de respectarea acestor principii şi poate demonstra această respectare (principiul responsabilității), precum și faptul că operatorul, potrivit art. 24, pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu regulamentul.

Raportat la cele expuse în adresă, s-a subliniat că datele nu pot fi dezvăluite de operatorii de date cu caracter personal autorități/instituții publice decât cu consimțământul persoanelor vizate sau dacă este îndeplinită una dintre celelalte condiții prevăzute de art. 6 alin. (1) din Regulamentul (UE) 2016/679, cu excepția situației prevăzute la lit. f) ("interes legitim") care nu se aplică în cazul prelucrării efectuate de autorități/instituții publice în îndeplinirea atribuțiilor lor.

Mai mult, s-a precizat că este necesar să fie luate în considerare și dispozițiile art. 6 alin. (4) din Regulamentul (UE) 2016/679 care instituie exigența compatibilității între scopul

inițial al prelucrării și cel ulterior și care trebuie să se reflecte în dreptul intern aplicabil operatorului, pentru a se institui garanții adecvate protejării drepturilor persoanelor vizate.

În ceea ce privește încheierea unui protocol de colaborare între societatea în cauză și instituții publice s-a atras atenția asupra bazei legale a transmiterii unor date personale între diverse entități publice, așa cum a statuat și Curtea de Justiție a Uniunii Europene în cauza C-201/14 (Smaranda Bara și alții împotriva Președintelui Casei Naționale de Asigurări de Sănătate și alții), "modalitățile de efectuare a transmiterii acestor informații au fost elaborate nu prin intermediul unei măsuri legislative, ci prin intermediul Protocolului din 2007 încheiat între ANAF și CNAS, care nu ar fi făcut obiectul unei publicări oficiale."

De asemenea, reafirmând importanța asigurării dreptului la informare, instanța UE a statuat faptul că: "... această cerință a informării persoanelor vizate de prelucrarea datelor lor cu caracter personal este cu atât mai importantă cu cât este o condiție necesară exercitării de către aceste persoane a dreptului lor de acces și de rectificare a datelor prelucrate, definit la articolul 12 din Directiva 95/46, și a dreptului de opoziție al acestora față de prelucrarea datelor respective, vizat la articolul 14 din această directivă." (pct. 33 din hotărâre).

În acest context, s-a subliniat că hotărârea instanței europene se aplică mutatis mutandis tuturor situațiilor în care autoritățile și instituțiile publice încheie protocoale între ele sau cu alte entități.

Totodată, s-a menționat că este necesar ca un operator de date cu caracter personal să analizeze, în funcție de specificul tuturor activităților efectiv realizate, toate prelucrările de date personale efectuate, să stabilească temeiul acestora și să ia toate măsurile necesare pentru asigurarea legalității prelucrării, pentru respectarea drepturilor persoanelor vizate, precum și pentru asigurarea securității și confidențialității datelor, raportat la prevederile legale din Regulamentul (UE) 2016/679.

- ***Legalitatea prelucrării de date din sistemul de supraveghere video al unei asociații de proprietari***

O asociație de proprietari a solicitat un punct de vedere cu privire la legalitatea accesării imaginilor din sistemul de supraveghere video al asociației de către membrii acesteia și publicarea anumitor imagini pe rețele de socializare, email și/sau la avizier.

Față de această solicitare, s-a precizat că dispozițiile art. 29 din Regulamentul (UE) 679/2016 menționează că: "Persoana împuternicită de operator şi orice persoană care acţionează sub autoritatea operatorului (de ex. angajatul operatorului) sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care dreptul Uniunii sau dreptul intern îl obligă să facă acest lucru."

Având în vedere dispozițiile de mai sus și ținând cont de principiul responsabilității operatorului (în speță, asociația de proprietari), s-a subliniat că este necesară stabilirea unui număr limitat de persoane care au acces la imagini. Totodată, s-a menționat că persoanele care au acces la imagini nu le prelucrează decât la cererea operatorului și în scopul pentru care datele au fost inițial colectate. Persoanele care au acces la imagini ar trebui să le poată vizualiza doar în situația producerii unui incident care are legătură cu scopul declarat al prelucrării, iar nu în mod continuu.

În același timp, s-a menționat că operatorul trebuie să asigure măsurile tehnice și organizatorice în conformitate cu art. 32 și art. 24 din Regulamentul (UE) 679/2016.

Astfel, la alin. (4) al art. 32 din Regulamentul (UE) 679/2016 se menționează că „Operatorul şi persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care această obligaţie îi revine în temeiul dreptului Uniunii sau al dreptului intern."

De asemenea, s-a menționat faptul că art. 5 din Regulamentul (UE) 679/2016 stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor. Printre acestea, se numără și cel privind prelucrarea datelor într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

Prin urmare, Autoritatea națională de supraveghere a subliniat că asociația de proprietari, în calitate de operator de date cu caracter personal, are responsabilitatea de a stabili modalitatea și mijloacele de acces la imaginile înregistrate de sistemul de supraveghere video, cu respectarea obligaţiilor stabilite de prevederile legale din

Regulamentul (UE) 679/2016 enunțate mai sus, în special a măsurilor privind confidențialitatea și securitatea datelor.

- ***Condiții legale de prelucrare a datelor cu caracter personal în contextul furnizării serviciilor medicale***

O unitate medicala privată a solicitat punctul de vedere al instituției noastre cu privire la temeiul legal al prelucrării datelor cu caracter personal în contextul furnizării serviciilor medicale.

Față de această solicitare, operatorului i s-au adus la cunoștință faptul că, în ceea ce privește modalitatea de prelucrare a datelor cu caracter personal, aceasta se realizează cu consimțământul persoanei vizate sau în condițiile de excepție de la consimțământ, prevăzute de art. 6 și art. 9 din Regulamentul (UE) 2016/679, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

Referitor la prelucrarea datelor privind starea de sănătate, petentul a fost informat că această prelucrare se supune prevederilor art. 9 din Regulamentul (UE) 2016/679. Astfel, prelucrarea acestei categorii de date cu caracter special se poate efectua când persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate.

Totodată, s-a subliniat că informarea persoanelor vizate trebuie realizată, indiferent de legitimitatea prelucrării datelor, respectiv la consimțământ sau în celelalte situații prevăzute de Regulamentul (UE) 2016/679, potrivit art. 13 sau 14 din Regulament, după caz, coroborat cu art. 12 din același regulament.

De asemenea, în contextul situației specifice expuse, s-a precizat că sunt aplicabile, printre altele, prevederile Legii nr. 95/2006 privind reforma în domeniul sănătății, republicată, cu modificările și completările ulterioare și ale Legii nr. 46/2003 privind drepturile pacientului.

Astfel, potrivit art. 660 din Legea nr. 95/2006, pentru a fi supus la metode de prevenție, diagnostic şi tratament, cu potențial de risc pentru pacient, după explicarea lor de către medic, medic dentist, asistent medical/moașă, pacientului i se solicită acordul scris.

Acordul scris al pacientului, necesar potrivit art. 660 alin. (3) din Legea nr. 95/2006 privind reforma în domeniul sănătăţii, republicată, cu modificările şi completările ulterioare, trebuie să conţină în mod obligatoriu cel puţin următoarele elemente:

a) numele, prenumele şi domiciliul sau, după caz, reşedinţa pacientului;

b) actul la care urmează a fi supus;

c) descrierea, pe scurt, a informaţiilor ce i-au fost furnizate de către medicul dentist;

d) acordul exprimat fără echivoc pentru efectuarea actului medical;

e) semnătura şi data exprimării acordului.

În acest context, s-a menționat că în funcție de scopul prelucrării datelor privind starea de sănătate sunt aplicabile prevederile Legii nr. 46/2003, ale Legii nr. 95/2006 coroborate cu Regulamentul (UE) 2016/679.

- ***Aplicarea Regulamentului (UE) 2016/679 în contextul instalării unui sistem de supraveghere video pe o proprietate privată***

Un petent a solicitat instituției noastre un punct de vedere cu privire la legalitatea instalării unui sistem de supraveghere video pe proprietatea sa.

Față de această solicitare, s-a precizat că prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor se supune, atât prevederilor Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, cât şi ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată.

Instalarea şi utilizarea sub aspect tehnic a echipamentelor şi elementelor componente ale sistemului de supraveghere video se realizează în conformitate cu Legea nr. 333/2003 şi normele metodologice de aplicare a acesteia.

Totodată, petentul a fost informat cu privire la prevederile art. 4 pct. 7 din Regulamentul (UE) 2016/679 care definesc „operatorul" ca fiind persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau

criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

Astfel, s-a menționat că, în situația în care sistemul de supraveghere video montat de o persoană fizică este orientat doar asupra propriului imobil ori bunului personal (curtea proprie, mașina personală, spre exemplu), pentru uzul exclusiv personal, sunt aplicabile prevederile art. 2 alin. 2 lit. c) din Regulamentul (UE) 2016/679, care exceptează de la aplicare prelucrările de date efectuate în scop personal sau domestic.

În sens contrar, în măsura în care sistemul de supraveghere video surprinde anumite părți din spațiul public, persoana fizică dobândește calitatea de operator de date cu caracter personal, raportat la prevederile Cauzei CJUE C-212/13, coroborat cu dispozițiile Regulamentul (UE) 2016/679.

Astfel, în Cauza CJUE C-212/13 Curtea de Justiție a Uniunii Europene a statuat că "în măsura în care o supraveghere video precum cea în discuție în litigiul principal se extinde, fie și parțial, la spațiul public și, în consecință, este îndreptată în afara sferei private a persoanei care efectuează prelucrarea datelor prin acest mijloc, aceasta nu poate fi considerată drept o activitate exclusiv „personală sau domestică" în sensul articolului 3 alineatul (2) a doua liniuță din Directiva 95/46."

De asemenea, petentul a fost informat că, în ceea ce privește imaginile captate și înregistrate de camerele video montate în zona de acces și zona perimetrală, în vederea respectării principiului proporționalității, se poate apela la echipamente care din punct de vedere tehnic pot fi orientate astfel încât să focalizeze doar zonele necesare a fi supravegheate.

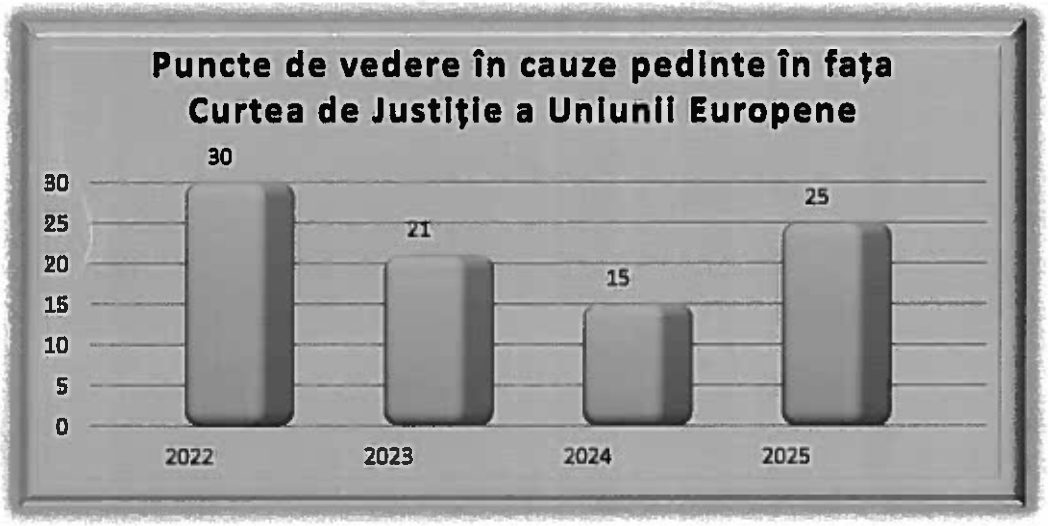
În plus, s-a subliniat că prelucrările de date efectuate vor fi precedate de o informare clară, concisă, într-un limbaj simplu, în conformitate cu art. 13 din R Regulamentul (UE) 2016/679.

Totodată, s-a precizat că în spațiile monitorizate trebuie instalată o pictogramă adecvată, care să conțină o imagine reprezentativă, poziționată la o distanță rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană. În acest sens, Autoritatea de supraveghere a recomandat ca perioada de stocare a datelor cu caracter personal (imaginea) prelucrate ca urmare a instalării sistemului de supraveghere video să nu depășească 30 zile.

În același timp, petentului i s-a adus la cunoștință faptul că operatorul trebuie să asigure măsurile tehnice și organizatorice în conformitate cu art. 32 și art. 24 din Regulamentul (UE) 2016/679.

## ■ Puncte de vedere privind unele cauze aflate pe rolul Curții de Justiție a Uniunii Europene

În anul 2025, Autoritatea națională de supraveghere a transmis către Ministerul Afacerilor Externe, puncte de vedere în **25 cauze** pendinte în fața Curții de Justiție a Uniunii Europene.




Cauzele analizate au avut ca obiect interpretarea anumitor articole din acte normative comunitare (Regulamentul (UE) 2016/679, Directiva 2016/680, Directiva 2002/58/CE, Directiva 2000/31/CE, Tratatul privind Funcționarea Uniunii Europene – TFUE), astfel:

- Cauza C-318/25 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la interpretarea dispozițiilor art. 267 din Tratatul privind Funcționarea Uniunii Europene;

- Cauza C-523/25 în cadrul căreia cererea a fost adresată de o instanță din Țările de Jos, referitoare la interpretarea prevederilor art. 80 alin. (1) și (2) din Regulamentul (UE) 2016/679;
- Cauza C-528/25 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la interpretarea dispozițiilor art. 13 alin. (3) și alin. (5) din Directiva 2002/58/CE;
- Cauza C-741/25 în cadrul căreia cererea a fost adresată de o instanță din Polonia referitoare la interpretarea dispozițiilor art. 15 alin. (1) din Directiva 2002/58/CE;
- Cauza E-5/25, aflată pe rolul Curții de Justiție a Asociației Europene a Liberului Schimb (AELS), în cadrul căreia cererea a fost adresată de o instanță din Liechtenstein referitoare la interpretarea art. 38 alin. (3), teza a doua din Regulamentul (UE) 2016/679;
- Cauza C-205/25 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la interpretarea dispozițiilor art. 4 pct. 7, art. 15 și art. 23 din Regulamentul (UE) 2016/679;
- Cauza C-302/25 în cadrul căreia cererea a fost adresată de o instanță din Austria referitoare la interpretarea dispozițiilor art. 1 alin. (6) din Directiva 2000/31/CE privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (Directiva privind comerțul electronic);
- Cauza C-317/25 în cadrul căreia cererea a fost adresată de o instanță din Franța referitoare la interpretarea dispozițiilor art. 4 pct. 11 din Regulamentul (UE) 2016/679, coroborat cu dispozițiile art. 13 și art. 14 din același regulament, precum și cu art. 13 din Directiva 2002/58/CE;
- Cauza C-12/25 în cadrul căreia cererea a fost adresată de o instanță din Belgia referitoare la interpretarea dispozițiilor art. 17, în mod particular, alin. (1) lit. (c) și alin. (3) lit. d) din Regulamentul (UE) 2016/679;
- C-185/25 în cadrul căreia cererea a fost adresată de o instanță din Austria referitoare la interpretarea dispozițiilor art. 4 pct. 7, art. 15 alin. (1) lit. g) și 82 alin. (1) din Regulamentul (UE) 2016/679;
- Cauza C-222/25 în cadrul căreia cererea a fost adresată de o instanță din Estonia, referitoare la interpretarea dispozițiilor art. 2 alin. (2) lit. d), art. 23 alin. (2) lit. h)

din Regulamentul (UE) 2016/679 și art. 2 alin. (1) coroborat cu art. 1 și art. 15 din Directiva nr. 680/2016;

- C-654/25 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la interpretarea dispozițiilor art. 4 pct. 1 și art. 82 alin. (1) din Regulamentul (UE) 2016/679;
- Cauza C-798/25 în cadrul căreia cererea a fost adresată de o instanță din Letonia referitoare la interpretarea dispozițiilor art. 14 lit. (d) punctul (i) și (ii) din Directiva nr. 1132/2017, raportat la art. 7 și art. 8 din Carta drepturilor fundamentale a Uniunii Europene, precum și art. 5 alin. (1) și, în mod particular, lit. (b) a art. 5 alin. (1) din Regulamentul (UE) 2016/679;
- Cauzele conexate C-124/25 și C-159/25 în cadrul căreia cererea a fost adresată de o instanță din Polonia referitoare la interpretarea dispozițiilor art. 2 și art. 19 alin. (1) al doilea paragraf din Tratatul privind Funcționarea Uniunii Europene coroborate cu art. 47 din Carta drepturilor fundamentale a Uniunii Europene și cu considerentul (61) al Regulamentului (UE) 2024/1689 de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828 (Regulamentul privind inteligența artificială);
- Cauza C-214/25 în cadrul căreia cererea a fost adresată de o instanță din Italia referitoare la interpretarea dispozițiilor art. 5 alin. (4) din Tratatul privind Funcționarea Uniunii Europene, precum și art. 5 alin. (1) lit. (b), (c) și (e) și art. 6 din Regulamentul (UE) 2016/679;
- Cauza C-568/25 în cadrul căreia cererea a fost adresată de o instanță din Austria referitoare la interpretarea dispozițiilor art. 22 alin. 2 lit. (a) din Regulamentul (UE) 2016/679;
- Cauza C-676/25 în cadrul căreia cererea a fost adresată de o instanță din Bulgaria referitoare la interpretarea dispozițiilor art. 8 din Carta Drepturilor Fundamentale a Uniunii Europene, art. 12 alin. 1 și 5 și ale art. 15 alin. 3 din Regulamentul (UE) 2016/679, coroborate cu considerentele (58) și (60) - (63) ale acestui regulament și cu Hotărârile Curții în cauzele C-487/21 și C-307/22, precum și art. 20 alin. (1) din Regulamentul (UE) 2016/679;

- Cauza preliminară C-427/25 în cadrul căreia cererea a fost adresată de o instanță din Italia referitoare la interpretarea dispozițiilor art. 15 alin. (1) din Directiva 2002/58/CE coroborat cu art. 7, art. 8, art. 11 și art. 52 din Carta Drepturilor Fundamentale a Uniunii Europene;
- Cauza preliminară C-458/25 în cadrul căreia cererea a fost adresată de o instanță din Belgia referitoare la interpretarea dispozițiilor art. 83 alin. (7) raportat la considerentele (38) și (58), și art. 6 alin. (1) lit. f), art. 8 și art. 57 alin. (1) lit. b) din Regulamentul (UE) 2016/679;
- Cauza preliminară C-416/25 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la interpretarea dispozițiilor art. 2 alin. (2) lit. d) din Regulamentul (UE) 2016/679, art. 1 alin. (1) și art. 2 alin. (1) din Directiva nr. 680/2016, raportat la dreptul național de transpunere a art. 56 și art. 14 din Directiva 680/2016 sau art. 82 coroborat cu art. 15 din Regulamentul (UE) 2016/679;
- Cauza preliminară C-594/25 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la interpretarea prevederilor art. 6 alin. (1) lit. f) și art. 82 alin. (1) și (2) din Regulamentul (UE) 2016/679.
- Cauza preliminară C-643/25 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la interpretarea dispozițiilor art. 4 pct. 1 și pct. 11, art. 7, art. 6 alin. (1) din Regulamentul (UE) 2016/679.

## ■ Puncte de vedere exprimate în contextul analizării evaluărilor de impact

• O entitate privată a transmis Autorității naționale de supraveghere, spre analiză *„Evaluarea impactului asupra protecției datelor (DPIA)"* în ceea ce privește instalarea la intrarea în spațiile de cazare a angajaților străini a unui sistem de identificare care se bazează pe amprentele digitale ale acestora.

Urmare a analizării evaluării de impact, raportat la activitățile desfășurate de operator, acestuia i s-a adus la cunoștință faptul că utilizarea biometriei ridică problema

proporționalității fiecărei categorii de date prelucrate, în lumina scopului în care sunt prelucrate acestea.

Astfel, sub aspectul proporționalității instituirii unei asemenea măsuri, operatorul a fost informat că, potrivit Avizului nr. 3/2012 privind progresele înregistrate de tehnologiile biometrice, emis de Comitetul European pentru Protecția Datelor "Utilizarea biometriei ridică problema proporționalității fiecărei categorii de date prelucrate în lumina scopului în care sunt prelucrate acestea. Având în vedere faptul că datele biometrice pot fi utilizate numai dacă sunt adecvate, relevante și neexcesive, trebuie să se evalueze cu exactitate necesitatea și proporționalitatea datelor prelucrate și să se analizeze dacă scopul urmărit ar putea fi atins într-un mod mai puțin intruziv."

De asemenea, operatorului i s-a comunicat că datele biometrice (amprentele digitale) pot fi prelucrate doar în condițiile prevăzute de art. 9 din Regulamentul (UE) 2016/679.

Totodată, Autoritatea națională de supraveghere i-a adus la cunoștință operatorului că, potrivit documentului intitulat "Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă" emis de Comitetul European pentru Protecția Datelor, "Angajații nu sunt aproape niciodată în măsură să își exprime, să refuze sau să își revoce în mod liber consimțământul, având în vedere dependența care rezultă din relația dintre angajator și angajat. Având în vedere dezechilibrul de puteri, angajații își pot da consimțământul liber numai în situații excepționale, atunci când nu există deloc consecințe legate de acceptarea sau respingerea unei oferte."

În acest context, Autoritatea națională de supraveghere a apreciat că, având în vedere natura sensibilă a datelor care necesită protecție, raportat la principiile legalității și proporționalității instituite de art. 5 și art. 9 din Regulamentul (UE) 2016/679, la condițiile de valabilitate a consimțământului prevăzute de art. 7 din același regulament, precum și aplicabilitatea acestora în relația angajat - angajator, situația prezentată nu se subsumează cerințelor de legalitate, necesitate și proporționalitate a prelucrării datelor biometrice.

În același timp, Autoritatea națională de supraveghere a considerat că este justificată necesitatea și proporționalitatea prelucrării de date biometrice ale propriilor angajați, prin raportare la scopul urmărit (accesul în spațiile de cazare ale angajaților străini ai operatorului prin intermediul unui sistem de verificare care se bazează pe "amprente

digitale"), fiind necesară alegerea unei alte soluții mai puțin intruzive pentru atingerea respectivului scop.

• Inspectoratului General al Poliției Române (IGPR) a supus atenției Autorității naționale de supraveghere un proiect al unei evaluări de impact asupra protecţiei datelor prelucrate în contextul introducerii de către IGPR a unui *"sistem de recunoaștere automată a numerelor de înmatriculare/înregistrare a autovehiculelor, de tip License Plate Recognition"* (sistem LPR).

În acelaşi timp, IGPR a comunicat Autorității naționale de supraveghere și proiectul de *"Dispoziție a Inspectorului general al Inspectoratului General al Poliției Române privind stabilirea regulilor de utilizare la nivelul structurilor Poliției Române a sistemului de recunoaștere automată a numerelor de înmatriculare/înregistrare a autovehiculelor (sistemul License Plate Recognition)".*

Autoritatea națională de supraveghere nu a avut alte observații față de versiunea modificată a documentului "Evaluarea impactului asupra protecției datelor a prelucrărilor de date personale efectuate de către Poliția Română, prin intermediul sistemului LPR", supus atenției instituției noastre și reanalizat prin raportare la dispozițiile Regulamentului (UE) 2016/679, Legii nr. 363/2018 și a celorlalte reglementări specifice aplicabile.

• Inspectoratului General al Poliției Române (IGPR) a supus atenției Autorității naționale de supraveghere *proiectul de "Evaluarea impactului asupra protecţiei datelor a operațiunilor de prelucrare efectuate de către Poliția Română, prin intermediul sistemului GPS"*.

Autoritatea națională de supraveghere a analizat documentele supuse atenției și a apreciat că proiectul de evaluare de impact transmis este întocmit în acord cu dispozițiile art. 35 - 36 din Regulamentul (UE) 2016/679, respectiv cu prevederile art. 30 - 34 din Legea nr. 363/2018. Ca atare, având în vedere:

- aspectele complexe privind prelucrările de date cu caracter personal legate de sistemul global de localizare prin satelit (sistem GPS), montat pe autovehiculele din dotarea I.G.P.R. și a instituțiilor subordonate, precum faptul că, în vederea implementării unui astfel de sistem, era necesar să se efectueze prelucrări de date care implică potențiale riscuri cu

privire la datele persoanelor fizice, angajați ai Poliției Române, care utilizează în cadrul activităților de serviciu desfășurate autovehiculele din dotare,

- proiectul de evaluare de impact - *"Evaluarea impactului asupra protecției datelor a operațiunilor de prelucrare efectuate de către Poliția Română, prin intermediul sistemului GPS"*, supus atenției Autorității naționale de supraveghere potrivit dispozițiilor art. 36 din Regulamentul (UE) 2016/679, respectiv art. 33 din Legea nr. 363/2018,

- proiectul de *dispoziție* a Inspectorului general al Inspectoratului General al Poliției Române privind stabilirea regulilor de utilizare pe autovehiculele Poliției Române a sistemului global de localizare prin satelit (GPS),

- recomandările Autorității naționale de supraveghere formulate operatorului IGPR față de conținutul proiectului de evaluare de impact ca, anterior începerii prelucrărilor preconizate a fi efectuate prin sistemul GPS, să ia în considerare următoarele:

■ corelarea mențiunii de la punctul 9 referitor la *"Potrivirea sau combinarea seturilor de date"* (pag. 6 din proiectul de evaluare de impact) cu mențiunea de la pag. 14 și pag. 16 referitoare la combinarea datelor despre locație cu alte date personale;

■ reanalizarea și corelarea mențiunilor de la pct. 10, 11 și 17 (pag. 6 din proiectul de evaluare de impact) referitoare la posibilitatea de exercitare a drepturilor de către persoanele vizate, angajați ai IGPR;

■ referitor la termenul de 3 ani stabilit pentru stocarea datelor, menționat la pag. 20 din proiectul de evaluare de impact, recomandăm reanalizarea acestuia, raportat la principiul "limitării legate de stocare" statuat în art. 5 alin. (1) lit. e) Regulamentul (UE) 2016/679;

■ cu privire la temeiurile legale de prelucrare a datelor angajaților IGPR prin intermediul sistemului global de localizare prin satelit (sistem GPS), montat pe autovehiculele din dotarea Poliției Române s-a recomandat:

a) reanalizarea menținerii ca temei de prelucrare a dispozițiilor art. 3, 4 și 5 din Ordonanța Guvernului nr. 27/2002 privind reglementarea activității de soluționare a petițiilor, cu modificările și completările ulterioare (pag. 29 din proiectul de evaluare de impact);

b) reanalizarea aspectelor referitoare la art. 5 din Legea nr. 190/2018 (pag. 31 și pag. 43 din proiectul de evaluare de impact), raportat la dispozițiile art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679, în contextul în care I.G.P.R., Direcția Generală de Poliție a

Municipiului București (D.G.P.M.B.) și inspectoratele de poliție județene (I.P.J.), aflate în subordinea I.G.P.R. (operatori de date care vor utiliza sistemul GPS) sunt autorități publice;

■ clarificarea aspectelor referitoare împuterniciți ai operatorului, în contextual în care la pag. 33 din evaluare există mențiunea conform căreia "Nu există persoane împuternicite de către operatori.", iar la pag. 41 din aceeași evaluare, la secțiunea "Contracte pentru remedierea deficiențelor cu persoana împuternicită de operator de date (conform art. 28 din RGPD)" sunt mențiuni referitoare la "remedierea defecțiunilor de către reprezentantul unei societăți cu care s-a încheiat anterior un contract (...)", și la secțiunea "Mecanisme de transfer și garanții" se face referire la "(...) reprezentantul tehnic al companiei care a implementat sistemul (...)",

- recomandările Autorității naționale de supraveghere de reanalizare a proiectului de dispoziție a Inspectorului general al Inspectoratului General al Poliției Române privind stabilirea regulilor de utilizare pe autovehiculele Poliției Române a sistemului global de localizare prin satelit (GPS),

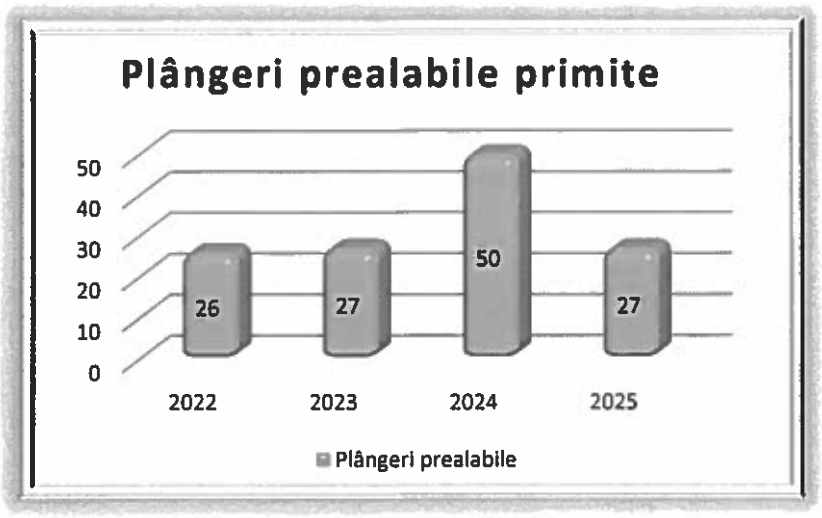
Autoritatea națională de supraveghere nu a formulat alte observații față de documentul "Evaluarea impactului asupra protecţiei datelor a operațiunilor de prelucrare efectuate de către Poliția Română, prin intermediul sistemului GPS", supus atenției instituției noastre și analizat prin raportare la dispozițiile Regulamentului (UE) 2016/679, Legii nr. 363/2018 și a celorlalte reglementări aplicabile.

## ■ Activitatea de soluționare a plângerilor prealabile

Potrivit art. 21 alin. (6) din Legea nr. 102/2005 privind înființarea, organizarea şi funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată, în măsura în care persoana vizată este nemulțumită de răspunsul primit ca urmare a depunerii unei plângeri la Autoritatea națională de supraveghere, aceasta se poate adresa secţiei de contencios administrativ a tribunalului competent, după parcurgerea procedurii prealabile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările şi completările ulterioare.

Astfel, în cursul **anului 2025,** au fost depuse la Autoritatea națională de supraveghere un număr de **27 plângeri prealabile.**

Dintre acestea, urmare a reanalizării susținerilor și documentelor suplimentare transmise de către petenți, **au fost admise 9 plângeri prealabile.**




## Secțiunea a 3 – a

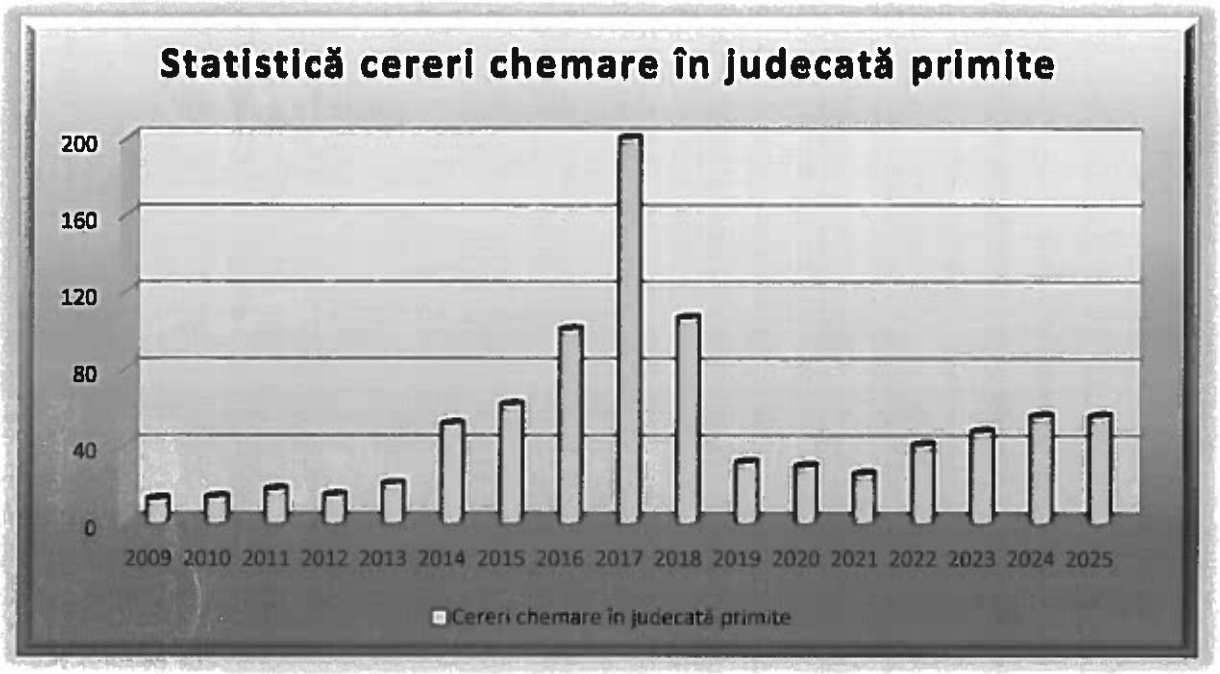
## Activitatea de reprezentare în fața instanțelor de judecată

**În anul 2025, Autoritatea națională de supraveghere a gestionat un număr de 195 dosare aflate pe rolul instanțelor de judecată în diferite stadii procesuale.**

Dintre acestea, **pe parcursul anului 2025** au fost înregistrate pe rolul instanțelor de judecată un număr de **55 de cereri noi de chemare în judecată**, întemeiate pe Regulamentul (UE) 2016/679 sau pe Legea nr. 554/2004 a contenciosului administrativ.

Menționăm că, **din cele 55** de cereri de chemare în judecată primite în anul 2025, **35 cereri de chemare în judecată** au avut ca **obiect contestarea proceselor – verbale de constatare/sancționare** încheiate de Autoritatea națională de supraveghere.

**Dintre litigiile care au avut ca obiect contestarea amenzilor în perioada 2019-2025, până în prezent au fost definitivate 55 dosare, iar dintre acestea în 47 de cauze au fost pronunțate soluții definitive în favoarea Autorității naționale de supraveghere.**




**În anul 2025 au fost finalizate definitiv mai multe acțiuni în mod favorabil pentru instituția noastră,** dintre care prezentăm mai jos câteva **litigii relevante**:

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea securității datelor cu caracter personal**

Autoritatea națională de supraveghere a efectuat o investigaţie ca urmare a unei plângeri prin care s-a reclamat faptul că au fost dezvăluite datele unei persoane vizate, aferente unei cereri de credit, către fostul soț, ca urmare a neactualizării în baza de date a băncii a datelor sale personale după divorț.

În cadrul investigației efectuate s-a constatat faptul că operatorul nu a adoptat suficiente măsuri de securitate, respectiv de a implementat măsuri tehnice şi organizatorice adecvate, incluzând capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea

și rezistența continue ale sistemelor și serviciilor de prelucrare, fapt care a condus la producerea încălcării de securitate prin transmiterea nesecurizată pe e-mail a datelor personale ale clientei băncii către o terță persoană, fiind astfel încălcate dispozițiile art. 32 din Regulamentul (UE) 2016/679.

De asemenea, în timpul investigației s-a constatat că operatorul nu a notificat Autorității naționale de supraveghere încălcarea de securitate cu toate că a luat la cunoștință de acest incident, fiind astfel încălcate și prevederile art. 33 din Regulamentul (UE) 2016/679.

Prin urmare, operatorul a fost sancționat contravențional cu amendă și avertisment, astfel:

- amendă în cuantum de 14.889 lei, echivalentul sumei de 3.000 euro, pentru încălcarea art. 32 din Regulamentul (UE) 2016/679 și

- avertisment pentru încălcarea art. 33 din Regulamentul (UE) 2016/679.

Autoritatea națională de supraveghere a aplicat și măsuri corective, dispunând operatorului următoarele:

- să asigure conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin punerea în aplicare a unor măsuri de securitate tehnice și organizatorice adecvate specificului prelucrării și riscurilor identificate, pe întreg ciclul de prelucrare a datelor, în special sub aspectul verificării exactității datelor personale prelucrate, al stabilirii unor reguli adecvate legate de redactarea și gestionarea fișierelor ce pot fi transmise prin folosirea mijloacelor de comunicare electronică (la distanță), al instruirii persoanelor care prelucrează date sub autoritatea sa, al verificării regulate a respectării instrucțiunilor transmise acestora, al automatizării anumitor procese prin care să fie reduse riscurile de prelucrare ilegală sau neautorizată a datelor personale;

- să asigure conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin adoptarea unor măsuri interne necesare pentru detectarea rapidă, gestionarea și raportarea unor situații de încălcare a securității datelor personale, (indiferent că ar necesita sau nu notificarea autorității de supraveghere și/sau a persoanelor vizate) precum și prin instruirea corespunzătoare și regulată a persoanelor care prelucrează date sub autoritatea operatorului.

Procesul-verbal de constatare/sancționare a fost contestat de operatorul sancționat.

Tribunalul București a reținut că *"(...) sancțiunea aplicată, reprezentând echivalentul a 3.000 de euro, a fost corect individualizată și nu se impune înlocuirea sa cu avertismentul, în raport de cuantumul maxim avut în vedere de legiuitor pentru sancțiunile aplicate față de nerespectarea dispozițiilor legale in materie de protecție a datelor cu caracter personal, fiind aplicată o amendă mult sub limita maximă stabilită de legiuitor.*

*De asemenea, tribunalul constată că reclamantei i s-a aplicat deja sancțiunea avertismentului atât pentru cealaltă, faptă constatată prin același proces-verbal de contravenție, cât și anterior, fiind sancționată cu avertisment pentru o altă faptă (...)'*.

În același timp, în mod corect a reținut instanța de fond și faptul că *„reclamanta nu a făcut dovada că a respectat prevederile art. 32 alin. (1) lit. b) din Regulamentul RGDP, prin transmiterea documentelor aferente cererii de credit la o adresă de e-mail anterioară a clientei, în condițiile în care, astfel cum rezultă din înscrisurile aflate la dosarul cauzei, în sistemul informatic al reclamantei se regăsea adresa nouă de e-mail a clientei (...), iar încă de la datele de 05.12.2018 și 01.07.2019 clienta a semnat formularul de actualizare a datelor cu caracter personal, în cuprinsul cărora era menționată noua adresă de e-mail (....).*

*Referitor la a doua faptă constatată în cuprinsul procesului-verbal de contravenție, sancționată cu avertisment pentru încălcarea disp. art. 33 din RGDP, tribunalul apreciază ca neîntemeiate apărările reclamantei, conform căreia situația de fapt se încadrează în excepția de la notificare, încălcarea securității datelor cu caracter personal fiind, in cazul de față, susceptibilă de a genera un risc pentru drepturile și libertățile persoanelor fizice."*

Prin hotărârea pronunțată, instanță de fond reține că *" (...) nu este lipsit de gravitate nici aspectul că informațiile au fost divulgate fostului soț al clientei, iar apărarea formulată de reclamantă, în sensul că în prezent clienta are o relație permanentă cu fostul soț prin prisma copiilor acestora, astfel că nu prezintă gravitate fapta săvârșită, vădește un total dezinteres al reclamantei față de valorile sociale ocrotite de norma incriminatoare și formează convingerea instanței că scopul educativ și preventiv al sancțiunii contravenționale nu poate fi atins decât prin menținerea amenzii în cuantumul aplicat de agent."*

Operatorul a formulat apel împotriva sentinței civile pronunțată de Tribunalul București.

Curtea de Apel București a respins apelul formulat de operator ca nefondat și, în mod corect, a reținut că *"Persistența reclamantei în săvârșirea unor fapte contravenționale*

*de aceeaşi natură nu poate fi neglijată, punând la îndoială capacitatea de conştientizare, integrare şi aplicare a obligaţiilor operatorului in domeniul datelor personale. În acest context este firească aplicarea şi menţinerea unei sancţiuni mai energice decât cea a avertismentului aplicată operatorului la prima abatere. În ce priveşte toate celelalte aspecte indicate de apelanta - reclamantă pentru a justifica un grad redus de pericol social al faptelor săvârşite, acestea au fost deja valorificate prin aplicarea unei sancţiuni cu amenda orientată către minim prin raportare la maximul posibil indicat in art. 83 din RGDP."*

**Ca atare, instanța de apel a respins definitiv, ca neîntemeiată, plângerea contravențională formulată de operatorul sancționat, confirmând abordarea Autorității naționale de supraveghere.**

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea prevederilor art. 4 alin. (5) din Legea nr. 506/2004 și art. 12-14 din Regulamentul (UE) 2016/679**

Autoritatea națională de supraveghere a efectuat o investigaţie ca urmare a unei sesizări cu privire la o posibilă încălcare a prevederilor Regulamentului (UE) 2016/679 și ale Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, modificată și completată.

Instituția noastră a fost sesizată cu privire la faptul că, prin intermediul site-ului deținut de un operator care activa în domeniul medical, nu se oferă posibilitatea accesării acestuia fără a accepta colectarea de informații prin tehnologiile cookies, respectiv fără consimțământul prealabil al utilizatorilor/vizitatorilor, și nici nu se asigură informarea persoanelor vizate conform prevederilor legale în domeniu.

În cursul investigației s-a constatat că operatorul permitea stocarea de informații și obținerea accesului la informațiile stocate pe echipamentele utilizatorilor prin folosirea fișierelor de tip cookies disponibile pe site-ul deținut, fără respectarea condițiilor legale privind obținerea prealabilă a consimțământului expres și informarea utilizatorilor, așa cum prevede art. 4 alin. (5) din Legea nr. 506/2004.

De asemenea, s-a constatat că operatorul nu asigura o informare completă a persoanelor vizate ale căror date personale le colecta și prelucra prin intermediul site-ului său, potrivit art. 12-14 din Regulamentul (UE) 2016/679.

Prin urmare, operatorul a fost sancționat contravențional cu o amendă și un avertisment, astfel:

- amendă în cuantum de 10.000 lei pentru încălcarea art. 4 alin. (5) din Legea nr. 506/2004;

- avertisment pentru încălcarea art. 12-14 din Regulamentul (UE) 2016/679.

Totodată, în sarcina operatorului s-au dispus și măsuri corective, astfel:

- să implementeze în mod activ prevederile art. 4 alin. (5) din Legea nr. 506/2004, prin raportare la dispozițiile art. 4 pct. 11, art. 7, art. 12-14 din Regulamentul (UE) 2016/679, prin obținerea consimțământului expres și informarea utilizatorilor, înainte de instalarea de cookies pe dispozitivul acestora, în cazul în care decide să folosească în continuare fișiere de tip cookies pe site-ul deținut;

- să asigure o informare completă a persoanelor vizate pe site-ul propriu, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, pe fiecare secțiune din site unde pot fi colectate/prelucrate date personale, prin raportare la dispozițiile art. 12-14 din Regulamentul (UE) 2016/679, informarea urmând să fie, în principal, în limba română.

Operatorul a contestat în instanță procesul–verbal de constatare/sancționare încheiat de Autoritatea națională de supraveghere.

Analizând probele cauzei, Tribunalului Cluj a respins plângerea formulată de operator.

În susținerile sale, instanța de fond a reținut faptul că *"(...) funcţionarea site-ului trebuie gândită astfel încât instalarea de cookie-uri să aibă loc doar în cazul în care utilizatorul şi-a dat acordul în acest sens şi numai după exprimarea acestui acord, ceea ce reclamanta nu a reuşit să asigure.*

*Sintetizând, tribunalul reține că site-ul administrat de către reclamantă permitea instalarea de cookie înainte ca utilizatorul să își exprime acordul în acest sens, fiind evident că erau încălcate prevederile art. 4 alin. (5) din Legea nr. 506/2004 și deci că s-a săvârșit contravenția prevăzută de art. 13 alin. (1) lit. i) din Legea nr. 506/2004."*

Tribunalul Cluj a mai arătat că *"reclamanta nu a administrat nicio probă din care să rezulte că aceleaşi informaţii erau oferite şi la momentul la care s-a constatat săvârşirea faptei contravenţionale. (...)".*

În ceea ce privește sancționarea operatorului pentru lipsa informării persoanelor vizate, în mod corect, instanța de fond reține: *"Din moment ce nu s-a furnizat nici o informaţie, încălcarea prevederilor art. 12 din RGPD este evidentă, astfel încât în mod corect s-a dispus sancționarea reclamantei pentru contravenția prevăzută la art. 12 din Legea nr. 190/2018 prin raportare la dispozițiile enumerate la art. 83 alin. (5) lit. b) din RGPD.*

*Pentru săvârşirea contravenţiei prevăzută de art. 13 alin. (1) lit. i) din Legea nr. 506/2004 reclamanta a fost sancționată potrivit regimului sancționator menţionat la art. 13 alin. (2) din Legea nr. 506/2004, care nu face trimitere la art. 83 din RGPD şi la criteriile reglementate aici, astfel încât acestea nu erau aplicabile."*

Totodată, cu privire la pericolul social și proporționalitatea sancțiunii aplicate de Autoritatea națională de supraveghere, instanța de fond, în mod just, reține că *"Sancţiunea trebuia aplicată conform art. 21 alin. (3) din OG 2/2001, care prevede că sancţiunea se aplică in limitele prevăzute de actul normativ și trebuie să fie proporţională cu gradul de pericol social al faptei săvârșite, ţinându-se seama de împrejurările în care a fost săvârșită fapta, de modul şi mijloacele de săvârşire a acesteia, de scopul urmărit, de urmarea produsă, precum şi de circumstanţele personale ale contravenientului şi de celelalte date înscrise in procesul-verbal. În ciuda susţinerilor reclamantei, fapta sa nu este lipsită de gravitate. Simpla împrejurare că reclamanta este la prima abatere nu este suficientă pentru a justifica înlocuirea amenzii cu avertisment, iar reclamanta nu a probat existenţa altor circumstanțe care să reflecte lipsa de gravitate a contravenţiei comise.*

*Tribunalul apreciază că sancţiunea aplicată reclamantei este proporţională cu fapta concretă reținută sarcina sa."*

Curtea de Apel Cluj a menținut hotărârea primei instanțe.

**Hotărârea judecătorească, favorabilă Autorității naţionale de supraveghere, a rămas definitivă.**

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea prevederilor prevederile art. 32 alin. (2) din Regulamentul (UE) 2016/679**

Autoritatea națională de supraveghere a efectuat o investigaţie ca urmare a unor sesizări prin care s-a reclamat faptul că persoane fizice, în calitate de consumatori, au posibilitatea să facă sesizări la un operator, instituție publică, prin utilizarea aplicației Whatsapp, sens în care instituția respectivă a postat pe site-ul său un comunicat de presă.

Potrivit comunicatului de presă, petenții acestui operator puteau sesiza nereguli cu caracter de urgență în raport cu nerespectarea drepturilor consumatorilor în ceea ce privește primirea unor facturi la energie electrică și gaze naturale, cazuri de debranșare pentru neplata unor facturi greșite la energie încă necorectate, precum și situații urgente care ar fi pus în pericol sănătatea consumatorilor, transmițând imagini și mesaje scrise în aplicația "WhatsApp" la un "număr special" de telefon.

În cadrul investigației efectuate s-a constatat faptul că operatorul a prelucrat nelegal datele cu caracter personal (imagini foto/video, număr de telefon, locația/aeroportul pe care se afla pasagerul, date cu caracter personal conținute în documente/înscrisuri precum facturi, bonuri, chitanțe - nume, prenume, domiciliu/punct de consum, număr de telefon, adresa), colectate prin utilizarea aplicației "WhatsApp", care nu se afla în controlul său, fără a ține seama, în special, de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod, fapt ce poate conduce la pierderea confidențialității datelor, prelucrarea neautorizată sau ilegală, pierderea, distrugerea sau deteriorarea accidentală, fiind încălcate astfel prevederile art. 32 alin. (2) din Regulamentul (UE) 2016/679.

Prin urmare, întrucât operatorul era instituție publică, acesta a fost sancționat cu avertisment, însoțit măsuri corective, menționate în planul de remediere anexat la procesul-verbal.

Procesul-verbal de constatare/sancționare a fost contestat de operatorul sancționat.

Tribunalului București, în mod corect, a respins contestația formulată ca neîntemeiată.

Pentru a hotărâ astfel, Tribunalul București a reținut că *„(...) reclamanta s-a adresat Autorităţii de supraveghere (...) cu privire la utilizarea aplicaţiei "WhatsApp" în contextul*

*comunicării cu consumatorii (persoane fizice), adică după 3 zile de la implementarea acestei aplicații (...). Or, reclamanta ar fi trebuit să se adreseze instituției pârâte anterior implementării aplicației. În plus, reclamanta avea posibilitatea să consulte propriul responsabil cu protecția datelor (...)"*

În susținerile sale, instanța de fond a constatat faptul că *„(...) la utilizarea unei aplicații de genul WhatsApp pentru transmiterea sesizărilor/reclamațiilor, tribunalul reține că această modalitate de comunicare cu consumatorii nu este prevăzută în niciun act specific domeniului de activitate al reclamantei (...)".*

Curtea de Apel București a respins apelul formulat de operator, ca nefondat.

Prin hotărârea pronunțată, instanța de apel a reținut că *„este de neînțeles cum apelanta a pus din nou la dispoziția consumatorilor această modalitate de transmitere a sesizărilor (...) deși intimata comunicase deja punctul de vedere al Autorității cu privire la utilizarea aplicației Whatsapp ca mod de comunicare cu consumatorii persoane fizice, în cadrul căruia a expus toate riscurile de securitate și a concluzionat că această prelucrare poate aduce o atingere gravă dreptului la viață privată și la protecția datelor persoanelor fizice (consumatorii) prin raportare la principiile de prelucrare, în special al legalității și al asigurării confidențialității și securității prelucrării datelor."*

Cu privire la individualizarea sancțiunii contravenționale, Curtea de Apel București a constatat că *„sunt întrunite elementele constitutive ale faptei imputate, contrar susținerilor apelantei, sancțiunea avertismentului fiind în mod legal aplicată de intimata-pârâtă prin procesul-verbal contestat, având în vedere dispozițiile art. 83 alin. 4 lit. a) din același Regulament care prevăd aplicarea unor amenzi administrative în cuantum maxim de 10.000.000 euro in cazul încălcării obligațiilor operatorului in conformitate cu art. 32."*

**Această hotărâre judecătorească, favorabilă Autorității naționale de supraveghere, a rămas definitivă.**

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea prevederilor art. 15 alin. (1), (2) și (3) și art. 12 alin. (2) din Regulamentul (UE) 2016/679**

Autoritatea națională de supraveghere a efectuat o investigație ca urmare a unei plângeri prin care s-a reclamat refuzul unui operator din domeniul financiar-bancar de a da curs integral cererii prin care un client (persoană fizică) și-a exercitat dreptul de acces, precum și omisiunea de a furniza anumite tipuri de informații în cadrul documentului "Politica Generală privind Protecția Datelor cu Caracter Personal".

În cadrul investigației efectuate Autoritatea națională de supraveghere a constatat că operatorul nu a prezentat dovezi din care să rezulte că a transmis un răspuns complet și particularizat la cererea formulată de client, prin raportare la datele și informațiile ce fac obiectul dreptului de acces prevăzut de art. 15 alin. (1) și (2) din Regulamentul (UE) 2016/679 încălcând, totodată, art. 15 alin. (3) din același regulament, întrucât nu i-a comunicat acestuia o copie a datelor personale prelucrate și nu i-a transmis răspunsul la adresa solicitată.

Autoritatea națională de supraveghere a constatat și că operatorul nu a adoptat măsuri prin care, în contextul exercitării dreptului de acces, să faciliteze accesul persoanelor vizate la copii ale înregistrărilor video ce le privesc și care sunt prelucrate de către operator, potrivit art. 12 alin. (2) din Regulamentul (UE) 2016/679, raportat la art. 15 alin. (3) și (4) din același regulament.

Prin urmare, operatorul a fost sancționat contravențional cu amenzi în cuantum total de 54.345 lei, echivalentul a 11.000 euro, astfel:

- amendă în cuantum de 4.940 lei, echivalentul a 1.000 euro pentru încălcarea art. 15 alin. (1), (2) și 15 alin. (3), respectiv a art. 12 alin. (4) coroborat cu art. 15 alin. (3) din Regulamentul (UE) 2016/679;

- amendă în cuantum de 49.405 lei, echivalentul a 10.000 euro pentru încălcarea art. 12 alin. (2) din Regulamentul (UE) 2016/679, raportat la art. 15 alin. (3) și (4) din același regulament.

Totodată, în sarcina operatorului s-au dispus și măsuri corective, și anume aceea de a răspunde la cererea petentului, prin comunicarea tuturor informațiilor prevăzute de art. 15 alin. (1) și (2) din Regulamentul (UE) 2016/679 și a copiei datelor personale prevăzute de art. 15 alin. (3) din același regulament, adaptate la situația specifică a acestuia, precum și măsura adoptării de măsuri tehnice și organizatorice adecvate, astfel încât să faciliteze exercitarea drepturilor persoanelor vizate, în special, a dreptului de acces la o copie a datelor lor personale ce fac obiectul prelucrării, inclusiv prin utilizarea unor programe

informatice care să permită editarea informațiilor de natură a aduce atingere drepturilor și libertăților altora.

Procesul-verbal de constatare/sancționare a fost contestat de operatorul sancționat.

Tribunalul București a reținut că "(...) *fapta contravențională există și a fost săvârșită de reclamantă, procesul-verbal contestat fiind temeinic.*"

De asemenea, în mod corect a reținut instanța de fond și faptul că *„În privința individualizării sancțiunii, instanța va reține că amenda contravențională a fost corect aplicată de către autoritatea pârâtă, în limitele prevăzute de lege. În același timp, sancțiunea este proporțională cu gradul de pericol social al faptei, iar tribunalul va avea în vedere că reclamanta nu este la prima abatere, așa cum a indicat în mod corect pârâtul."*

Operatorul a formulat apel împotriva sentinței pronunțate de tribunal.

**Curtea de Apel București a respins definitiv, ca neîntemeiată, plângerea contravențională formulată de operatorul sancționat, confirmând abordarea Autorității naționale de supraveghere.**

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea măsurilor de securitate**

Autoritatea națională de supraveghere a efectuat o investigație ca urmare a transmiterii de către un operator a unei notificări de încălcare a securității datelor cu caracter personal, în temeiul art. 33 din Regulamentul (UE) 2016/679.

În cadrul investigației s-a constatat că încălcarea securității datelor s-a produs ca urmare a divulgării neautorizate a datelor cu caracter personal (ID, adresa, nume, prenume, adresa de e-mail, companie, vânzări, activ, abonat la buletinul informativ, înregistrare și ultima vizită) pentru un număr semnificativ de clienți ai operatorului, aceste date fiind accesibile pe site-ul acestuia.

Totodată, Autoritatea națională de supraveghere a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prezentat de prelucrare, generat în special, de divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal stocate.

Operatorul a fost sancționat cu amendă în cuantum de 14.904 lei, echivalentul a 3.000 EURO, pentru încălcarea prevederilor art. 32 alin. (1) lit. a), b) și d), coroborat cu art. 32 alin. (2) din Regulamentul (UE) 2016/679.

În temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, s-au dispus următoarele măsuri corective împotriva operatorului:

- implementarea unui plan care să includă un proces de testare, evaluare și apreciere periodică ale tuturor sistemelor și modificărilor ulterioare ale acestora efectuate de operator sau furnizorii de servicii (persoane împuternicite), în special asupra site-ului administrat de operator;

- elaborarea și implementarea unor proceduri de complexitate a parolelor, în special pentru conturile de administrator, care să cuprindă cerințe specifice privind: lungimea minimă a parolei, varietatea caracterelor, perioada de expirare a acesteia, precum și imposibilitatea reutilizării unei parole înregistrate anterior.

Operatorul a contestat în instanță procesul–verbal de constatare/sancționare încheiat de Autoritatea națională de supraveghere.

Analizând probele cauzei, Tribunalului Timiș a respins plângerea formulată de operator.

În mod corect, Tribunalul Timiș, analizând întreg materialul probator administrat în cauză, prin prisma dispozițiilor legale incidente și a susținerilor părților, a reținut că *"În primul rând, (...) reclamantul nu a formulat critici din perspectiva legalității și temeiniciei procesului-verbal contestat, susținând doar că ar fi intervenit prescripția dreptului pârâtei de a aplica sancțiunea amenzii contravenționale, având în vedere dispozițiile art. 13 din OG nr. 2/2001 privind regimul juridic al contravențiilor, care prevăd un termen de prescripție de 6 luni de la data săvârșirii faptei."*

Tribunalul Timiș *"(...) constată că art. 15 alin. (4) din Legea nr. 102/2005 prevede un termen de prescripție derogatoriu de la O.G. nr. 2/2001, respectiv: „(4) Sancțiunile prevăzute la alin. (1) pot fi aplicate în termen de 3 ani de la data săvârșirii faptei. În cazul încălcărilor care durează în timp sau al celor constând în săvârșirea, în baza aceleiași rezoluții, la intervale diferite de timp, a mai multor acțiuni sau inacțiuni, care prezintă, fiecare în parte, conținutul aceleiași contravenții, prescripția începe să curgă de la data constatării sau de la data încetării ultimului act ori fapt săvârșit, dacă acest moment intervine anterior constatării".*

*În aceste condiții, tribunalul va respinge ca neîntemeiată apărarea reclamantului privind intervenirea prescripției dreptului pârâtei de a aplica sancțiunea amenzii contravenționale."*

În ceea ce privește contestarea modalității în care Autoritatea națională de supraveghere a aplicat dispozițiile legate cu privire la individualizarea sancțiunii, în mod corect Tribunalul Timiș *"(...) reține, pentru început, că odată cu intrarea in vigoare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), operatorii de date și persoanele împuternicite de operatori au dobândit responsabilități sporite în vederea protejării eficace a datelor cu caracter personal ale persoanelor. În același timp autoritățile de supraveghere au competența de a garanta că principiile prevăzute in Regulamentul general privind protecția datelor, precum și drepturile persoanelor fizice în cauză sunt apărate, în conformitate cu litera și spiritul Regulamentului, aplicarea consecventă a normelor în materie de protecție a datelor fiind esențială pentru un regim de protecție a datelor armonizat. Amenzile administrative sunt un element central în cadrul noului sistem de punere în aplicare introdus de Regulament, fiind o componentă importantă a setului de instrumente de aplicare ale autorităților de supraveghere, împreună cu celelalte măsuri prevăzute la articolul 58.*

*La fel ca toate măsurile corective alese de autoritățile de supraveghere, amenzile administrative trebuie să fie „eficace, proporționale și disuasive" și să țină seama in mod corespunzător de natura, gravitatea și consecințele încălcării, iar autoritățile de supraveghere trebuie să evalueze toate circumstanțele speței într-un mod coerent și justificat în mod obiectiv.*

*Evaluarea a ceea ce este eficace, proporțional și disuasiv în fiecare caz trebuie să reflecte, de asemenea, obiectivul urmărit de măsura corectivă aleasă, și anume fie să restabilească conformitatea cu normele, fie să sancționeze un comportament ilegal (sau ambele).*

*Articolul 83 alineatul (2) din Regulament prevede o listă de criterii pe care autoritățile de supraveghere sunt obligate să le utilizeze atât pentru evaluarea oportunității aplicării unei amenzi, cat și pentru evaluarea cuantumului acesteia.*

*Aproape toate obligaţiile operatorilor şi ale persoanelor împuternicite de operatori în conformitate cu Regulamentul sunt clasificate, in funcţie de natura lor, în cadrul dispoziţiilor articolului 83 alineatele (4) - (6).*

*Regulamentul, prin stabilirea a două cuantumuri maxime diferite ale amenzilor administrative (10.000.000 Euro/20.000.000 Euro), indică deja că o încălcare a anumitor dispoziţii din regulament poate fi mai gravă decât în cazul altor dispoziţii."*

În ceea ce privește speța dedusă judecății, în mod corect a reținut Tribunalul Timiș că *"În cazul de faţă reclamantul a fost sancționat în temeiul art. 83 alin. (4) lit. a) din Regulament, pentru încălcări ale prevederilor art. 32 alin. (1) si (2) din Regulament, amenda stabilită fiind în cuantum de 14.904,30 lei (echivalentul a 3.000 euro); limita maxima a sancţiunii amenzii prevăzută de art. 83 alin. (4) lit. a), este in sumă de 10.000.000 de euro.*

*În ceea ce priveşte natura încălcării, Tribunalul reține că reclamantul nu a implementat măsuri tehnice şi organizatorice adecvate în scopul asigurării unui nivel de securitate corespunzător riscurilor. (...)*

*Tribunalul subliniază că Regulamentul a introdus un nivel mult mai ridicat de responsabilizare a operatorului de date în comparație cu Directiva 95/46/CE privind protecţia datelor, iar articolele 25 şi 32 din Regulament prevăd că operatorii „au in vedere stadiul actual al tehnologiei, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice pe care le prezintă prelucrarea".*

În ceea ce privește consecinţele încălcării, Tribunalul Timiș reține *"că acestea au fost corect calificate de către pârâtă ca fiind grave, prin raportare la numărul persoanelor vizate afectate (800) şi la durata încălcării (...).*

*Pârâta a valorificat corespunzător şi criteriile prevăzute la art. 83 alin. (2) lit. c) - k), dovada examinării temeinice a acestor criterii fiind tocmai stabilirea unei amenzi într-un cuantum mult inferior maximului admis pentru fapta săvârșită de reclamant. De altfel, procesul-verbal cuprinde în detaliu analiza efectuată de pârâtă cu privire la fiecare dintre criteriile stabilite prin art. 83 alin. (2) din Regulament pentru individualizarea sancţiunii.*

*Tribunalul nu poate reține ca fiind o circumstanță atenuantă, care să justifice aplicarea unui avertisment, împrejurarea că reclamantul este cel care a notificat Autoritatea despre incidentul de securitate, în condiţiile in care art. 33 din Regulament stabileşte în mod expres obligaţia operatorului de date de a notifica Autoritatea de supraveghere in cazul*

*încălcării securității datelor cu caracter personal. Mai mult, faptul de a nu notifica Autoritatea de supraveghere reprezintă o contravenție distinctă, potrivit art. 83 alin. (4) lit. a) din Regulament. Tribunalul mai reține că reclamantul nu și-a îndeplinit obligația de notificare a Autorității în termenul prevăzut de lege (72 de ore de la data la care a luat cunoștință de încălcarea securității datelor cu caracter personal).*

*Pentru toate considerentele de fapt și de drept mai sus expuse, tribunalul concluzionează în sensul că amenda în cuantum de 14.904,30 lei (echivalentul a 3.000 euro) este legală, eficace, proporțională și disuasivă și a fost stabilită cu luarea în considerare a naturii, gravității și consecințelor încălcării, precum și a tuturor celorlalte criterii prevăzute de Regulament, criterii care au fost analizate de pârâtă în mod coerent si obiectiv."*

Având in vedere aceste argumente, tribunalul a respins ca neîntemeiată contestația formulată de reclamant împotriva procesului verbal de constatare/sancționare.

**Curtea de Apel Timiș a respins definitiv, ca neîntemeiată, plângerea contravențională formulată de operatorul sancționat, dând câștig de cauză instituției noastre.**

## Secțiunea a 4-a:
## Informare publică

**Autoritatea națională de supraveghere a continuat, în anul 2025, activitățile de comunicare destinate informării publicului larg, cu privire la regulile de prelucrare a datelor cu caracter personal, în contextul Regulamentului (UE) 2016/679.**

În acest sens, prezentăm succint cele mai relevante dintre aceste manifestări:

♦ **Ziua Europeană a Protecției Datelor – 28 Ianuarie 2025**

Pe data de 28 ianuarie 2025 se celebrează Ziua Europeană a Protecției Datelor de către toate statele membre ale Consiliului Europei, când s-au împlinit 44 de ani de la adoptarea Convenției 108 pentru protecția persoanelor referitoare la prelucrarea

automatizată a datelor cu caracter personal, de către Consiliul Europei, primul instrument juridic în domeniu.

În anul 2025, în considerarea semnificației speciale a acestui an pentru instituția noastră și a Zilei Europene a Protecției Datelor, Autoritatea națională de supraveghere a organizat, pe data de 28 ianuarie 2025, Conferința on-line intitulată *„Bilanț aniversar la 20 de ani de la înființarea ANSPDCP".*

Autoritatea națională de supraveghere a sărbătorit în 2025 împlinirea a 20 de ani de la adoptarea, pe data de 3 mai 2005, a Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

La acest eveniment organizat de Autoritatea națională de supraveghere au participat reprezentanți ai autorităților și instituțiilor publice centrale naționale, ai forului executiv și legislativ, reprezentanții mediilor academice, organizațiilor nonguvernamentale, ai principalelor uniuni/asociații profesionale, precum și operatori/împuterniciți relevanți din sectorul public și privat.

Cu acest prilej, au fost aduse în atenția invitaților implicațiile utilizării noilor tehnologii, fiind accentuat gradul de conștientizare a publicului larg asupra riscurilor utilizării neadecvate a datelor personale și necesitatea respectării dreptului la viață privată a persoanelor, în contextul inovării digitale accelerate și a impactului asupra prelucrărilor de date cu caracter personal.

În același timp, Autoritatea națională de supraveghere a pregătit și pus la dispoziția publicului, pe pagina proprie de internet www.dataprotection.ro, **materialele informative** (broșuri, pliante) dedicate Zilei Europene a Protecției Datelor, precum și informații privind activitatea din anul anterior.

De asemenea, în contextul derulării acestui eveniment, pe postul național de televiziune TVR și în mijloacele de transport ale Societății de Transport București, a fost difuzat **clipul informativ** dedicat Regulamentului (UE) 2016/679 – mesaj de interes public, referitor la principalele aspecte reglementate de Regulamentul (UE) 2016/679, realizat de instituția noastră.

♦ **Moment aniversar – Împlinirea a șapte ani de la aplicarea Regulamentului (UE) 2016/679 – 25 Mai 2025**

Cu prilejul sărbătoririi a șapte ani de la aplicarea Regulamentului (UE) 2016/679 pe site-ul instituției a fost postat un comunicat de presă ce prezintă o sinteză a celor mai importante aspecte din activitatea Autorității naţionale de supraveghere, desfășurată pe parcursul primelor patru luni ale anului 2025.

Din datele statistice analizate, a rezultat faptul că s-a continuat activitatea de monitorizare și control cu privire la legalitatea prelucrărilor de date personale, care a vizat, în principal, următoarele aspecte:

- dezvăluirea datelor personale către terți în spațiul public, în mediul on-line;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video;
- nerespectarea drepturilor persoanelor vizate;
- primirea de mesaje comerciale nesolicitate:
- încălcarea principiilor de prelucrare a datelor.

Pentru aceeași perioadă analizată, a rezultat faptul că Autoritatea națională de supraveghere a emis un număr semnificativ de **puncte de vedere** ca răspuns la solicitările operatorilor și împuterniciților acestora (din domeniul public și privat), precum și din partea altor entități și a persoanelor fizice, privind diverse aspecte referitoare la modalitatea de aplicare a Regulamentului (UE) 2016/679 și a celorlalte reglementări incidente.

În aceeași perioadă, au fost emise avize asupra unor proiecte de acte normative transmise de instituţii publice, ceea ce a implicat analizarea unor aspecte diverse și complexe privind aplicarea adecvată a regulilor de protecție a datelor în mai multe domenii de activitate specifice și a fost continuată activitatea de reprezentare în instanță, și cea de comunicare destinate informării publicului larg, cu privire la regulile de prelucrare a datelor cu caracter personal.

♦ **Conferințe, seminare, reuniuni**

Instituţia noastră a participat activ și în anul 2025 la cele mai semnificative conferințe și **reuniuni pe plan național,** cu incidență în domeniul protecției datelor, organizate de diverse instituții publice sau de entități private.

În cadrul acestor evenimente, reprezentanții Autorității naţionale de supraveghere au clarificat aspecte privind condiții de prelucrarea a datelor, respectarea drepturilor persoanelor vizate în situații specifice, asigurarea confidenţialităţii și protecției datelor cu caracter personal, ceea ce reflectă continuitatea deschiderii către publicul larg.

Pe data de 23 ianuarie 2026 a avut loc *Conferința Data Privacy Observer*, organizată de Universul Juridic, în cadrul căreia a avut loc și o intervenție privind constatările Autorității naționale de supraveghere referitoare la aplicarea regulilor de protecția datelor personale

În luna martie 2025 , reprezentanții Autorității naționale de supraveghere au susținut un seminar de instruire a polițiștilor din cadrul Inspectoratului General al Poliției Române, în cadrul căruia au fost reliefate constatările relevante din activitatea de control și recomandări privind desfășurarea activității.

Totodată, reprezentanții Autorității naționale de supraveghere au participat la o **serie de reuniuni și întâlniri, atât cu reprezentanți ai altor autorități publice, precum și cu cei din sectorul privat, astfel:**

- Autoritatea Națională pentru Protecția Consumatorilor a organizat o întâlnire în vederea clarificării anumitor aspecte privind competențele instituțiilor în contextul comerțului electronic și al aplicării Regulamentului (UE) 2022/2065 privind o piaţa unică pentru serviciile digitale şi de modificare a Directivei 2000/31/CE (Regulamentul privind serviciile digitale);

- Institutul Național de Statistică a solicitat o întrevedere cu experții instituției noastre ocazie cu care au avut loc discuții privind proiectul de Lege privind registrul statistic de populație;

- Agenția Națională de Integritate, în calitate de autoritate desemnată cu monitorizarea aplicarea prevederilor Legii nr. 361/2022 privind protecția avertizorilor în interes public, cu modificările ulterioare, a organizat o întâlnire în vederea clarificării anumitor aspecte;

- Consiliul Concurenței a solicitat o întrevedere în vederea clarificării anumitor aspecte privind prelucrări de date cu caracter personal efectuate de entități ale căror activități sunt supuse unor investigații declanșate de Consiliului Concurenței și care au ca obiect posibila încălcare a prevederilor art. 6 alin. (1) din Legea concurenței nr. 21/1996, republicată, cu modificările și completările ulterioare, și a prevederilor art. 102 alin. (1) din Tratatul privind Funcționarea Uniunii Europene;

- Asociația Română a Băncilor și membrii ai acesteia – discuții în perspectiva finalizării de către Asociația Română a Băncilor a Codului de Conduită al Asociației;

- Autoritatea pentru Digitalizarea României – reuniune cu autoritățile competente referitoare la aplicarea Regulamentului privind inteligența artificială;

- Senatul României a lansat "Strategia Națională pentru Prevenirea și Tratarea Dependenței de Jocuri de Noroc", document elaborat de Oficiul Național pentru Jocuri de Noroc, în care se recunoaște dependența de jocuri de noroc ca un risc major pentru sănătatea publică care necesită intervenții precoce și care reprezintă un plan coordonat pentru gestionarea riscurilor de adicție, bazat pe fonduri colectate anual de la operatorii de jocuri.

- O firmă de avocatură a organizat "Privacy & Innovation Forum", eveniment la care au fost puse în discuție, în principal, impactul Regulamentului (UE) 2016/679 și al Directivei ePrivacy asupra inovației, modul în care inteligența artificială (AI) poate fi un element care facilitează sau un blocaj pentru afaceri, provocările cu privire la conformitate în peisajul digital aflat în continuă schimbare.

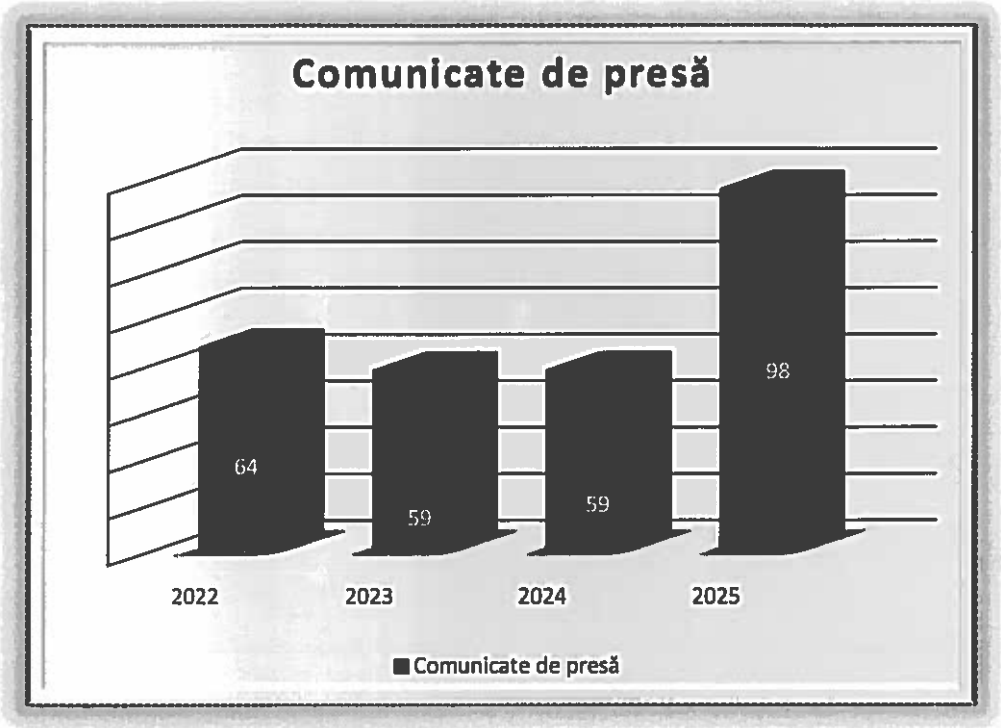
De asemenea, au fost puse în discuție preconizatele modificări ale Regulamentului (UE) 2016/679 propuse prin pachetul Omnibus VII, care face parte dintr-o agendă mai largă a Uniunii Europene de a face legislația mai ușor de aplicat pentru întreprinderi și autorităţi, în sensul simplificării normelor europene în domeniul digital, reducerii sarcinii administrative și consolidării suveranității digitale.

Pe de altă parte, subliniem că instituția noastră a realizat o informare promptă şi eficientă a operatorilor din mediul public și privat, precum și a persoanelor fizice, prin intermediul **audiențelor** acordate la sediul Autorității naţionale de supraveghere.

În același timp, prin intermediul celor **aprox. 3.000 de consultații telefonice**, în cadrul programului zilnic de relații cu publicul, cu privire la modalitatea practică de aplicare a prevederilor Regulamentului (UE) 2016/679, au fost explicitate și clarificate o serie de măsuri pe care operatorii sunt obligați să le implementeze în vederea respectării dispozițiilor acestui Regulament.

♦ **Site-ul Autorității naţionale de supraveghere**

Autoritatea naţională de supraveghere a realizat și în cursul anului 2025 o informare promptă şi eficientă cu privire la activitatea desfășurată, atât prin prisma celor **98 de comunicate de presă** postate pe site-ul instituției noastre la secțiunea „Știri", cât și a informațiilor de la secțiunea specială dedicată Regulamentului (UE) 2016/679.




**Față de aspectele prezentate mai sus, putem concluziona că instituția noastră a utilizat instrumentele existente pentru a asigura o informare adecvată a publicului larg, inclusiv a operatorilor, în condițiile resurselor bugetare și umane existente.**

# CAPITOLUL III

# ACTIVITATEA DE MONITORIZARE ȘI CONTROL

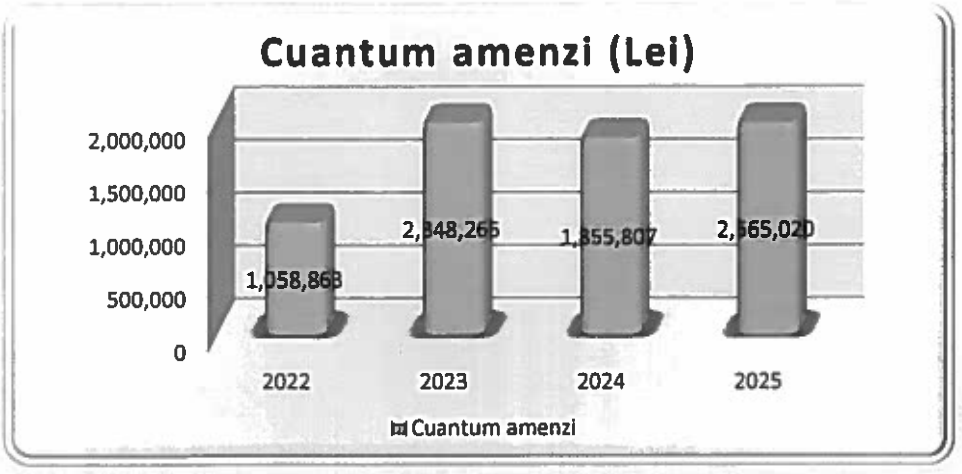
## Secțiunea 1: Prezentare generală

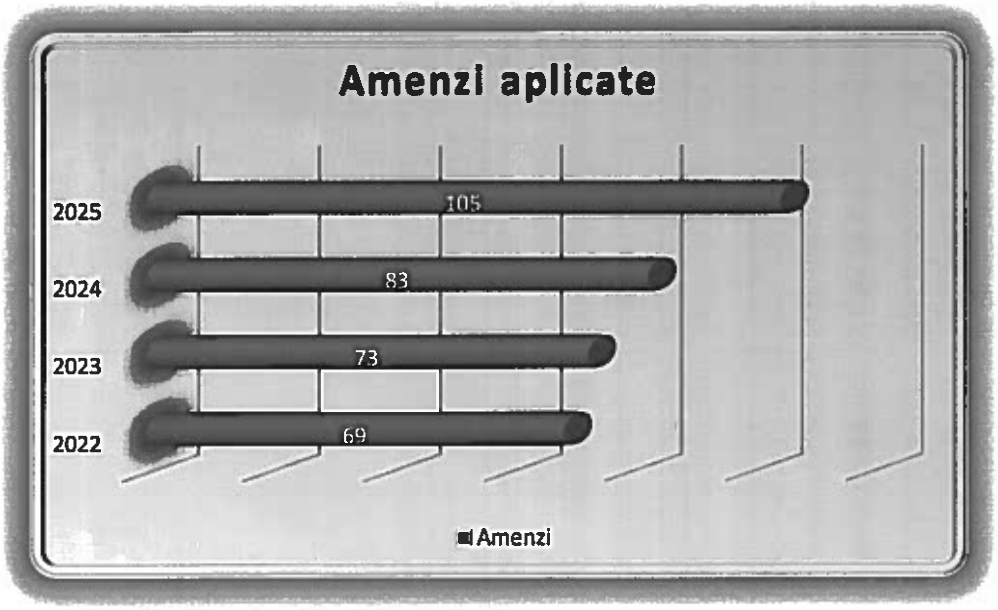
**În cursul anului 2025**, Autoritatea Națională de Supraveghere a primit un număr de 12.297 de plângeri, sesizări și notificări privind incidente de securitate. De asemenea, în anul 2025 au fost finalizate **488 investigații**.




Ca urmare a investigațiilor efectuate, Autoritatea Națională de Supraveghere a aplicat, în anul 2025, în total **105 de amenzi** în cuantum total **de 2.565.020,37 lei - echivalentul sumei de 511.400 euro.**

Dintre acestea, **96 de amenzi** au fost aplicate în baza Regulamentului (UE) 2016/679 (în cuantum **de 2.378.020,37 lei**) și **9 amenzi** au fost aplicate în baza Legii nr. 506/2004 (în cuantum de **187.000 lei).**




De asemenea, în cursul anului 2025, au mai fost aplicate în total **145 de avertismente**, au fost dispuse **182 de măsuri corective, 3 avertizări** și au fost emise **5 decizii.**




**Principalele aspecte rezultate în urma analizării plângerilor primite de Autoritatea națională de supraveghere în cursul anului 2025 au fost următoarele:**

- prelucrarea datelor cu caracter personal cu nerespectarea principiilor legalității, echității și transparenței, precum și a condițiilor de legalitate prevăzute la art. 5 și art. 6 din Regulamentul (UE) 2016/679;
- încălcarea drepturilor persoanelor vizate, în special a dreptului de acces și a dreptului la ștergerea datelor, inclusiv în cadrul Sistemului de Informații Schengen (SIS);
- transmiterea de materiale și mesaje electorale către persoane fizice;
- blocarea sau restricționarea accesului la conturi de pe rețelele de socializare;
- divulgarea neautorizată a datelor cu caracter personal către terți, inclusiv prin intermediul rețelelor de socializare, al platformelor online, cât și la avizier;
- prelucrarea datelor cu caracter personal prin intermediul sistemelor de supraveghere video;
- transmiterea de comunicări comerciale nesolicitate prin e-mail, telefon sau alte mijloace de comunicare;
- raportarea și prelucrarea datelor cu caracter personal în cadrul Biroului de Credit;
- prelucrarea datelor în domeniul jocurilor de noroc;
- încălcarea obligațiilor privind securitatea și confidențialitatea prelucrărilor de date cu caracter personal.

**Referitor la încălcarea securității datelor cu caracter personal, în cursul anului 2025, notificările transmise Autorității naționale de supraveghere au vizat, în principal, următoarele aspecte:**

- confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare a dezvăluirilor neautorizate prin transmiterea eronată de date cu caracter personal;
- confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare ca urmare a incidentelor informatice de tip atac ransomware sau infectarea sistemelor cu fișiere malițioase;
- confidențialitatea datelor cu caracter personal în mediul online ca urmare a gradului insuficient de securizare informatică la nivelul site-urilor și aplicațiilor informatice utilizate de operatori;
- confidențialitatea datelor cu caracter personal prin nerespectarea principiului privacy by design/privacy by default, ca urmare a testării insuficiente a aplicațiilor informatice anterior lansării în mediul de producție, respectiv monitorizarea implicită a acestora în mediul de producție;
- prelucrarea datelor cu caracter personal ale clienților din sistemul bancar;
- accesul neautorizat la sistemele de supraveghere video cu circuit închis.

**Prin intermediul sesizărilor transmise în anul 2025 au fost semnalate, în principal, aspecte referitoare la:**

- configurare greșită a aplicațiilor care utilizează baze de date cu caracter personal în sensul expunerii publice a acestora prin intermediul serviciului de world wide web, cu sau fără indexarea acestora de către motoarele de căutare;
- implementarea unui sistem de control al accesului pentru angajați, bazat pe date biometrice (amprentă digitală);
- supravegherea/monitorizarea video a propriilor angajați;
- intenția operatorului de a implementa un sistem de recunoaștere facială (date biometrice);

- divulgarea prin transmitere a unor rezultate genetice/genomice ale pacienților către alte entități medicale;
- prelucrarea datelor cu caracter personal colectate prin intermediul camerelor video de tip body-cam fără a exista o obligație legala a operatorului și fără îndeplinirea vreunei alte condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679;
- încălcarea legalității prelucrării datelor cu caracter personal ca urmare a transmiterii pe e-mail a unor copii ale actelor de identitate ale mai multor angajați;
- încălcarea principiilor de prelucrare a datelor prevăzute de Regulamentul (UE) 2016/679;
- dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;
- confidențialitatea datelor cu caracter personal în mediul on-line ca urmare a configurării deficitare a site-urilor sau aplicațiilor informatice utilizate;
- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale prin neadoptarea de către operatori a măsurilor tehnice și organizatorice adecvate privind asigurarea securității prelucrărilor.

## Secțiunea a 2-a: Investigații din oficiu

### I. Prezentare generală

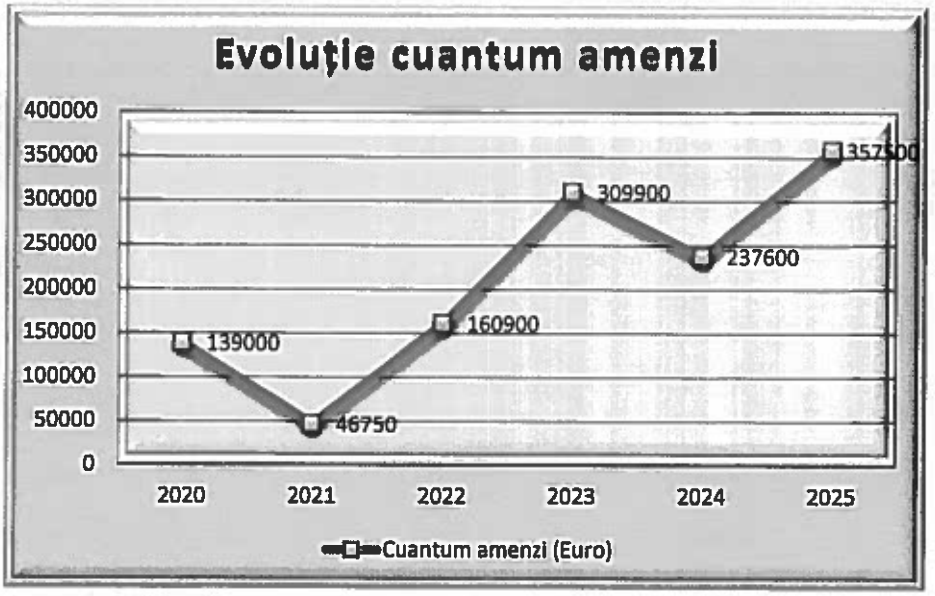
În cursul anului 2025, a continuat activitatea de monitorizare și control a operatorilor din sectorul public și privat, urmărindu-se cu prioritate obiective legate de respectarea prevederilor Regulamentului (UE) 2016/679, ale Legii nr. 190/2018, dar și ale Legii nr. 506/2004.

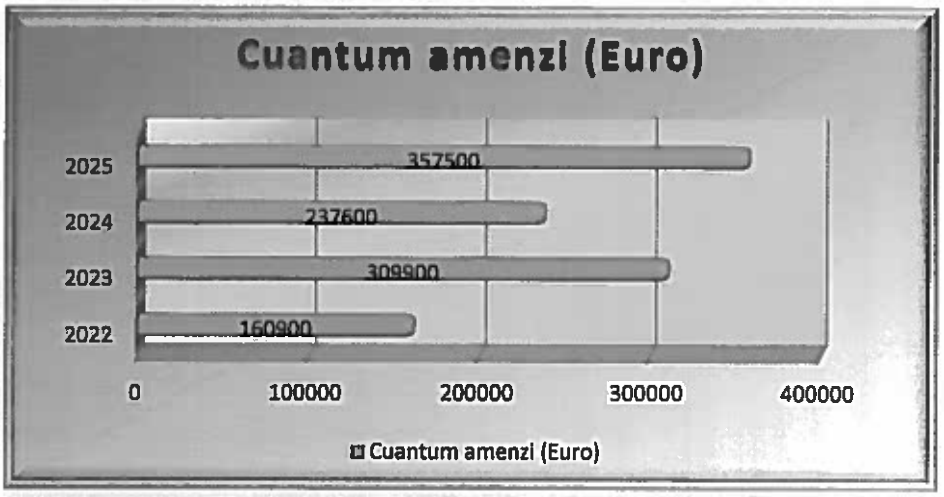
În anul 2025, Autoritatea națională de supraveghere a primit un număr total de **1019 sesizări și notificări** de încălcare a securității datelor cu caracter personal, dintre care **814 sesizări și 205 încălcări de securitate a datelor cu caracter personal** (202 încălcări ale Regulamentului (UE) 2016/679 și 3 încălcări ale Legii nr. 506/2004).




În cursul anului 2025, Autoritatea națională de supraveghere a finalizat un număr de **312 investigații** din oficiu. Urmare a investigațiilor efectuate în anul 2025, au fost aplicate:

- **50 de amenzi** în baza **Regulamentului (UE) 2016/679**, în cuantum total de **1.813.894 lei** (echivalentul sumei de **357.500 euro**);
- **8 amenzi** în baza Legii nr. 506/2004, în cuantum total de **182.000 lei**;






De asemenea, în investigațiile din oficiu efectuate au fost aplicate **54 avertismente**, **3 avertizări, 4 decizii** și au fost dispuse **64 măsuri corective**.




În anul 2025, prin intermediul **sesizărilor** transmise au fost semnalate, în principal, aspecte referitoare la:

- configurarea greșită a aplicațiilor care utilizează baze de date cu caracter personal în sensul expunerii publice a acestora, cu sau fără indexarea acestora de către motoarele de căutare;

- implementarea unui sistem de control al accesului pentru angajați, bazat pe date biometrice (amprentă digitală);
- supravegherea/monitorizarea video a propriilor angajați;
- intenția operatorului de a implementa un sistem de recunoaștere facială;
- divulgarea prin transmitere a unor rezultate genetice ale pacienților către alte entități medicale decât operatorul;
- prelucrarea datelor cu caracter personal colectate prin intermediul camerelor video de tip body-cam, fără a exista o obligație legală a operatorului și fără îndeplinirea altei condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679;
- încălcarea legalității prelucrării datelor cu caracter personal ca urmare a transmiterii pe e-mail a unor copii ale actelor de identitate ale mai multor angajați;
- încălcarea principiilor de prelucrare a datelor prevăzute de Regulamentul (UE) 2016/679;
- dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;
- confidențialitatea datelor cu caracter personal în mediul on-line ca urmare a configurării deficitare a site-urilor sau aplicațiilor informatice utilizate de operatori;
- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale.

**Referitor la încălcarea securității datelor cu caracter personal**, în cursul anului 2025, **notificările** transmise Autorității naționale de supraveghere **au vizat**, în principal, următoarele aspecte:

- confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare a dezvăluirilor neautorizate prin transmiterea eronată de date cu caracter personal;
- confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare ca urmare a incidentelor informatice de tip atac ransomware sau infectarea sistemelor cu fișiere malițioase;
- încălcarea confidențialității datelor cu caracter personal în mediul online ca urmare a gradului insuficient de securizare informatică la nivelul site-urilor și aplicațiilor informatice utilizate de operatori;

- încălcarea confidențialității datelor cu caracter personal prin nerespectarea principiului privacy by design/privacy by default, ca urmare a testării insuficiente a aplicațiilor informatice anterior lansării în mediul de producție, respectiv lipsa monitorizării implicite a acestora în mediul de producție;
- prelucrarea datelor cu caracter personal ale clienților din sistemul bancar;
- accesul neautorizat la sistemele de supraveghere video cu circuit închis.

**Măsurile corective dispuse în urma investigațiilor din oficiu** au vizat, în special, următoarele:

- implementarea tehnică și organizatorică a unui proces de testare, evaluare și apreciere periodică a tuturor acțiunilor de introducere/actualizare date cu caracter personal pentru persoanele vizate;
- informarea regulată privind riscurile prelucrării neautorizate a datelor cu caracter personal de către angajați prin diseminarea acestei informări;
- implementarea unor sisteme de monitorizare/jurnalizare a accesului în infrastructura IT utilizată pentru prelucrarea datelor cu caracter personal care să includă o perioadă de retenție a log-urilor de acces de minim 30 zile, inclusiv introducerea unui proces de backup asupra acestora;
- efectuarea unei evaluări de impact asupra datelor cu caracter personal raportat la prevederile Deciziei nr. 174/2018 a Autorității naționale de supraveghere;
- implementarea tehnică și organizatorică a unor măsuri de diminuare a riscului încălcării confidențialității datelor cu caracter personal prin atac informatic.

### A. Investigații referitoare la prelucrarea datelor cu caracter personal de către entități din domeniul privat

În anul 2025, investigațiile din oficiu la entitățile private s-au desfășurat ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal și a sesizărilor cu privire la prelucrarea datelor cu caracter personal.

Notificările de încălcare a securității datelor cu caracter personal transmise de entitățile private au vizat, în principal:

- divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal prelucrate, în special în mediul online sau ca urmare a unui incident informatic de tip atac ransomware;
- neimplementarea unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- neimplementarea unor măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, în special în domeniul financiar-bancar;
- încălcarea confidențialității datelor cu caracter personal în mediul online ca urmare a configurării deficitare a site-urilor sau aplicațiilor informatice utilizate de operatori;
- accesul neautorizat la sistemele de supraveghere video cu circuit închis.

De asemenea, sesizările referitoare la activitatea de prelucrare a datelor cu caracter a entităților private au avut ca obiect, în principal, divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal, încălcarea principiilor de prelucrare a datelor prevăzute de Regulamentul (UE) 2016/679, dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate, precum și încălcarea confidențialității datelor cu caracter personal în mediul on-line.

Ca urmare a investigațiilor efectuate au fost aplicate operatorilor atât sancțiuni contravenționale, cât și măsuri corective.

**1. FIȘĂ DE CAZ - Divulgarea neautorizată sau accesul neautorizat la date cu caracter personal**

În baza mecanismelor de cooperare prevăzute de Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere, în calitate de autoritate de supraveghere principală, a finalizat o investigație la un operator, în cadrul căreia a constatat încălcarea dispozițiilor art. 32 alin. (1) lit. b) și d) și alin. (2) din Regulamentul (UE) 2016/679.

Ca atare, operatorul a fost sancționat contravențional cu amendă în cuantum de 35.615 lei (echivalentul sumei de 7.000 euro).

Investigația a fost demarată ca urmare a transmiterii de către operator a unei notificări cu privire la încălcarea securității datelor cu caracter personal, potrivit dispozițiilor art. 33 din Regulamentul (UE) 2016/679, precum și ca urmare a unei sesizări primite de Autoritatea națională de supraveghere.

Astfel, încălcarea de securitate a vizat un acces neautorizat la sistemul de gestionare a contractelor operatorului. Din notificarea transmisă Autorității naționale de supraveghere a rezultat că incidentul a fost raportat cu întârziere pe cale internă, fapt pentru care la nivelul operatorului nu ar fi fost luate imediat măsuri necesare și adecvate, ceea ce a condus la afectarea datelor cu caracter personal a unui număr semnificativ de persoane vizate, inclusiv din alte state membre ale Uniunii Europene.

În cadrul investigației s-a constatat faptul că încălcarea de securitatea s-a produs ca urmare a faptului că un fost angajat a divulgat credențialele unor colegi pentru sistemul de gestionare a contractelor, fapt ce a permis accesul neautorizat la datele cu caracter personal (nume, prenume, adresă, număr de telefon, email, locul și data nașterii, număr și dată de expirare permis de conducere, serie și număr CI/pașaport, CNP) unui număr semnificativ de persoane vizate, inclusiv persoane vizate din state membre UE/Spațiul Economic European și Non UE.

Ca atare, s-a stabilt că operatorul a încălcat prevederile art. 32 alin. (1) lit. b) și d) și alin. (2) din Regulamentul (UE) 2016/679, întrucât nu a pus în aplicare măsuri tehnice și organizatorice adecvate fapt ce a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal unui număr foarte mare de clienți persoane fizice și angajați ai acestuia.

În acest context, raportat la implicațiile transfrontaliere ale situației, operatorul a fost sancționat cu amendă printr-o decizie emisă de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, potrivit competențelor instituite de Regulamentul (UE) 2016/679 și Legea nr. 102/2005, republicată.

În același timp, Autoritatea națională de supraveghere a aplicat și măsura corectivă prin care s-a dispus ca operatorul să implementeze o procedură de revocare a drepturilor de acces și dezactivare a conturilor asociate foștilor angajați.

Operatorul a achitat amenda contravențională stabilită.

## 2. FIȘĂ DE CAZ - Divulgarea neautorizată sau accesul neautorizat la date cu caracter personal prin accesarea codului sursă a aplicației operatorului

Autoritatea națională de supraveghere a finalizat, în anul 2025, o investigație la un operator (partid politic) și a constatat încălcarea prevederilor:

a) art. 32 alin. (1) lit. b) și d) și alin. (2) din Regulamentul (UE) 2016/679, coroborat cu art. 25 alin. (1) și (2) din același act normativ;

b) art. 5 alin. (1) lit. c) și alin. (2), raportat la dispozițiile art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Pentru faptele săvârșite s-au aplicat operatorului următoarele sancțiuni:

a) amendă, în cuantum de 50.587 lei, echivalentul sumei de 10.000 euro

b) amendă, în cuantum de 75.880 lei, echivalentul sumei de 15.000 euro

Investigația a fost demarată ca urmare a transmiterii de către operator a două notificări cu privire la încălcarea securității datelor cu caracter personal, potrivit dispozițiilor art. 33 din Regulamentul (UE) 2016/679, precum și ca urmare a unor sesizări primite de Autoritatea națională de supraveghere.

a) Una dintre încălcările de securitate notificată a vizat aplicația mobilă utilizată și gestionată de operator a cărei vulnerabilitate a fost exploatată de un terț prin accesarea codului sursă a aplicației.

În cadrul investigației s-a constatat faptul că, urmare a unei greșeli de configurare, la momentul producerii incidentului puteau fi vizualizate în cadrul aplicației următoarele categorii de date cu caracter personal ale utilizatorilor acesteia (susținători/membri persoane fizice care au furnizat date cu caracter personal în aplicația operatorului): numele și prenumele, numărul de telefon, adresa de e-mail, adresa de reședință, codul numeric personal, data nașterii, naționalitatea, cetățenia, sexul, religia, profesia, ocupația, domeniul de activitate, experiența în alte domenii, studiile (instituție, specializare, dată început, dată sfârșit), experiența politică (partid, funcție, dată început, dată sfârșit), experiența administrativă (instituție, funcție, dată început, dată sfârșit), limbile străine vorbite (limbă, nivel).

Prin urmare, s-a constatat că operatorul a încălcat prevederile art. 32 alin. (1) lit. b) și d) și alin. (2), coroborat cu art. 25 alin. (1) și (2) din Regulamentul (UE) 2016/679,

întrucât acesta nu a pus în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane, incluzând capacitatea de a asigura confidențialitatea și rezistența continue ale sistemelor și serviciilor de prelucrare, precum și un proces pentru testarea, evaluarea şi aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării, respectiv nu a implementat, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, astfel de măsuri tehnice și organizatorice adecvate.

Aceasta a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale utilizatorilor aplicației (susținători/membrii ai partidului), prin accesarea codului sursă a aplicației de către persoane terțe, ca urmare a interogării unei interfețe de programare vulnerabile.

b) Autoritatea Electorală Permanentă a redirecționat Autorității naționale de supraveghere două sesizări prin care era semnalată o posibilă încălcare a prevederilor Regulamentului (UE) 2016/679 de către operator, prin colectarea de date cu caracter personal (nume, prenume, serie și număr CI, adresa de domiciliu, data nașterii, email, număr de telefon, semnătură) prin intermediul a două platformele online, pentru un număr semnificativ de persoane vizate.

În cadrul investigației s-a constatat faptul că datele cu caracter personal erau prelucrate de operator în scopul informării persoanelor vizate cu privire la o campanie a operatorului, și în scop statistic, precum și că datele prelucrate nu sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile declarate ale prelucrării.

Ca atare, s-a stabilit că operatorul a încălcat prevederile art. 5 alin. (1) lit. c) și alin. (2) din Regulamentul (UE) 2016/679 prin raportare la dispozițiile art. 6 alin. (1) din Regulament, întrucât a prelucrat fără temei legal, prin intermediul platformelor online, date cu caracter personal care nu sunt adecvate, relevante și limitate la ceea ce este necesar, în raport cu scopurile declarate ale prelucrării.

În timpul investigației operatorul a dezactivat platformele informatice.

### 3. FIȘĂ DE CAZ – Atac informatic asupra unei platforme de e-commerce pentru produse din tutun, executat prin exploatarea unor vulnerabilități ale acesteia

Un operator din domeniul comercializării produselor din tutun a notificat, conform art. 33 din Regulamentul (UE) 2016/679, o încălcare a securității datelor cu caracter personal prin transmiterea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Decizia nr. 128/2018.

Autoritatea națională de supraveghere a constatat, în cadrul investigației efectuate, că operatorul nu a adoptat măsuri de securitate adecvate în vederea asigurării confidențialității datelor prelucrate, ceea ce a condus la încălcarea securității datelor cu caracter personal.

Incidentul a condus la divulgarea neautorizată a datelor cu caracter personal (de ex. număr card bancar, numele și prenumele deținătorului de card, data expirării cardului) pentru un număr semnificativ de persoane vizate, în urma unui atac informatic desfășurat asupra platformei de e-commerce a operatorului, prin redirecționarea clienților către o pagină de plată frauduloasă.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 101.544 lei, echivalentul sumei de 20.000 de euro, pentru încălcarea art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679.

De asemenea, s-a dispus măsura corectivă de implementare tehnică și organizatorică a unui sistem de jurnalizare a tuturor accesărilor asupra platformei de e-commerce a operatorului, cu reținerea acestora pe o durată de cel puțin 120 zile, inclusiv cu efectuarea de back-up asupra fișierelor de jurnalizare (log-uri).

### 4. FIȘĂ DE CAZ – Pierderea confidențialității datelor cu caracter personal prelucrate de un operator prin intermediul unui atac cibernetic

Un operator a notificat o încălcare a securității datelor cu caracter personal, constând în accesarea neautorizată, prin intermediul unui atac informatic, a datelor cu caracter personal ale unui număr semnificativ de angajați ai operatorului.

În cadrul investigației derulate, Autoritatea națională de supraveghere a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prezentat de prelucrare, generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal.

Incidentul a rezultat în divulgarea neautorizată a datelor cu caracter personal (nume angajat, numărul intern de angajat, email-ul de birou, departamentul, titulatura interna, adresa biroului operatorului în care lucrează, data creării contului angajatului, codul de țară) ale unui număr semnificativ de persoane vizate la nivelul UE, prin intermediul unui atac informatic executat prin exploatarea vulnerabilității unor parole și a modalității de resetare a autentificării unui cont de utilizator compromis.

Autoritatea națională de supraveghere a apreciat faptul că circumstanțele cazului prezintă un grad de gravitate accentuat care impune aplicarea unei sancțiuni cu amendă împotriva operatorului, raportat la criteriile de individualizare a amenzilor prevăzute la art. 83 din Regulamentul (UE) 2016/679 și a dispus, prin decizie, aplicarea unei amenzi în cuantum de 50.899,00 lei, echivalentul sumei de 10.000 euro.

Autoritatea de supraveghere nu a dispus măsuri corective operatorului, considerând adecvate măsurile adoptate de acesta ulterior incidentului notificat.

**5. FIȘĂ DE CAZ – Prelucrarea ilegală a imaginii prin mijloace de supraveghere video la locul de muncă**

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că la nivelul unei societăți a fost accesat neautorizat sistemul de supraveghere video și ulterior s-au utilizat înregistrările video ale angajaților în scopul efectuării unor cercetării disciplinare.

În cadrul investigației efectuate Autoritatea națională de supraveghere a constatat faptul că operatorul nu a putut prezenta dovezi cu privire la respectarea principiilor și a condițiilor de legalitate prevăzute de Regulamentul (UE) 2016/679, precum și ale condițiilor prevăzute de art. 5 din Legea nr. 190/2018, care să permită operatorului utilizarea mijloacelor de supraveghere video pentru monitorizarea propriilor angajați la locul de muncă și, implicit, prelucrarea imaginii acestora de către angajator în contextul derulării unei cercetări disciplinare.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 24.887 RON, echivalentul a 5.000 EURO pentru încălcarea art. 5 alin. (1) lit. a) și b), alin. (2) din Regulamentul (UE) 2016/679, raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679 și art. 5 din Legea nr. 190/2018, în temeiul art. 58 alin. (2) lit. i) și 83 alin. (5) lit. a) din Regulamentul (UE) 2016/679.

De asemenea, s-a dispus măsura corectivă de asigurare a conformității operațiunilor de prelucrare a datelor personale în activitatea de monitorizare video, în special în cazul efectuării de cercetări disciplinare ale angajaților, cu respectarea principiilor și a condițiilor de prelucrare prevăzute de art. 5 și art. 6 din Regulamentul (UE) 2016/679, respectiv de art. 5 din Legea nr. 190/2018.

Operatorul a contestat procesul - verbal de constatare/sancționare.

**6. FIȘĂ DE CAZ – Prelucrarea datelor biometrice din cadrul unei societăți cu activitate de jocuri de noroc**

În urma primirii mai multor petiții cu privire la intenția unei societăți cu activitate de jocuri de noroc de a implementa un sistem de securitate bazat pe recunoaștere facială (date biometrice) pentru accesul propriilor angajați, Autoritatea națională de supraveghere a demarat o investigație la operatorul respectiv.

În cadrul investigației desfășurate, Autoritatea națională de supraveghere a constatat că prelucrarea datelor biometrice, prin utilizarea unui sistem de recunoaștere facială destinat identificării persoanelor care accesează spațiile operatorului (precum angajați, furnizori sau vizitatori), în scopul prevenirii accesului neautorizat, al evitării utilizării necorespunzătoare a cardurilor de acces sau al partajării legitimațiilor, este susceptibilă să contravină dispozițiilor art. 5 alin. (1) lit. a) și c), coroborate cu art. 6 din Regulamentul (UE) 2016/679. S-a apreciat că o asemenea prelucrare poate aduce atingere dreptului la viață privată și dreptului la protecția datelor cu caracter personal ale persoanelor vizate.

În acest context, Autoritatea națională de supraveghere a sancționat operatorul cu avertizare, în temeiul art. 58 alin. (2) lit. a) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 15 alin. (2) din Legea nr. 102/2005, republicată.

Operatorul s-a conformat avertizării emise de către Autoritatea națională de supraveghere și nu a procedat la punerea în aplicare a sistemului de prelucrare a datelor biometrice, aflat în evaluare internă la data investigației.

**7. FIȘĂ DE CAZ – Divulgarea datelor cu caracter personal prin intermediul unui site**

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, prin intermediul unui site care aparține unei societăți comerciale, sunt publicate date cu caracter personal ale persoanelor fizice autorizate. Societatea a declarat faptul că deține acele date din informațiile publicate de către Oficiului Național al Registrului Comerțului, Agenția Națională de Administrare Fiscală și Ministerul Finanțelor.

În urma investigației, Autoritatea națională de supraveghere a constatat faptul că operatorul a încălcat prevederile art. 5 alin. (1) lit. a) și alin. (2) și art. 6 din Regulamentul (UE) 2016/679, deoarece a prelucrat datele cu caracter personal (nume, prenume, data înființării, adresă) prin afișarea acestora pe site-ul respectiv, deși societatea avea obligația de a prelucra datele cu caracter personal în mod legal, echitabil și transparent față de persoana vizată și de a demonstra această responsabilitate.

Astfel, instituția noastră a sancționat entitatea privată cu avertisment, pentru încălcarea art. 5 alin. (1) lit. a) și alin. (2) și art. 6 din Regulamentul (UE) 2016/679.

În urma constatărilor și a sancționării societății de către Autoritatea națională de supraveghere, aceasta a dezactivat site-ul respectiv.

**8. FIȘĂ DE CAZ – Divulgarea și accesul neautorizat la date**

Un operator cu activitate comercială a notificat o încălcare a confidențialității datelor cu caracter personal ale angajaților săi conținute în nota de calcul a drepturilor salariale (nume, prenume, locul muncii, număr de marcă intern angajat, câștiguri salariale, rețineri și contribuții salariale, inclusiv cotizație sindicat, pentru un anumit număr de membri sindicat, ore lucrate, concedii, delegații, seminarii, cheltuieli sociale, contribuții pensii facultative, popriri, asigurare suplimentară de sănătate, zile donații sânge, vouchere de vacanță).

În fapt, în urma implementării modalității de comunicare electronică a acestor note de calcul prin e-mail, un număr semnificativ de fișiere a ajuns la alte persoane decât destinatarii, angajați ai operatorului.

Incidentul a fost generat de rularea concomitentă a mai multor sesiuni de lucru asupra aceluiași fișier PDF. În aceste condiții, aplicația a primit comenzi simultane de generare a acestor note de calcul, comenzi provenite din sesiuni diferite, deschise în conturile a doi utilizatori cu drepturi de acces depline și nerestricționate (angajați ai departamentului de resurse umane, responsabili cu transmiterea acestora). Ca urmare a acestor solicitări simultane de generare a notelor de calcul, programul nu a putut procesa în mod corespunzător datele aferente.

Autoritatea națională de supraveghere a reținut, urmare a investigației efectuate la operator, precum și la împuternicitul acestuia (furnizorul aplicației), că operatorul nu a avut cerințe specifice de dezvoltare și testare multisesiune cu privire la aplicația furnizată de împuternicitul său.

De asemenea, s-a reținut că operatorul nu a furnizat persoanei împuternicite instrucțiuni conform cărora se dorește transmiterea notelor de calcul în regim multisesiune și nici nu a solicitat în momentul testării efective a aplicației un astfel de scenariu.

Urmare a investigației efectuate, operatorul a fost sancționat cu amendă în cuantum de 15.109 lei, echivalentul în lei a sumei de 3000 euro, pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și d) și alin. (2) din Regulamentul (UE) 2016/679, deoarece nu a implementat măsuri organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, având în vedere riscurile prezentate de prelucrare pentru drepturile și libertățile persoanelor fizice vizate, precum și un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării, cum ar fi testarea aplicației în regim multisesiune într-un mediu de test, fapt ce a condus la divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal ale unui număr semnificativ de angajați ai operatorului, prin rularea modulului de transmitere a notelor de calcul a drepturilor salariale într-un scenariu netestat anterior (de tip multisesiune), direct în mediul de producție.

## 9. FIȘĂ DE CAZ – Divulgarea și accesul neautorizat la datele cu caracter personal prelucrate prin intermediul aplicațiilor utilizate

Un operator din domeniul industriei alimentare a notificat o încălcare a confidențialității, integrității și disponibilității datelor cu caracter personal generată de un atac cibernetic de tip ransomware.

Atacul a avut drept consecință întreruperea activităților de producție și gestionare a stocurilor, procesele de livrare, logistică și administrative, accesul la baza de date a clienților și la sistemele de management și contabil, sistemele informatice esențiale devenind inaccesibile.

În fapt, atacatorul a avut acces la date și documente din infrastructura informatică a operatorului utilizând credențialele unui utilizator.

Urmare a investigației demarate, Autoritatea națională de supraveghere a reținut că operatorul nu a implementat măsuri de securitate adecvate, nu a utilizat soluții eficiente de protecție antivirus/antimalware, nu a aplicat mecanisme de securitate la nivelul dispozitivelor individuale și nici nu a implementat o soluție centralizată pentru monitorizarea amenințărilor de securitate.

Autoritatea națională de supraveghere a constatat, urmare a investigației efectuate, că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării. Aceasta a condus la accesul neautorizat la datele cu caracter personal prelucrate de operator pentru un număr mare de persoane vizate (angajați și clienți).

Operatorul a fost sancționat cu amendă în cuantum de 25.226 lei, echivalentul sumei de 5.000 euro, pentru încălcarea art. 32 alin. (1) lit. b) și d) și alin. (2) din Regulamentul (UE) 2016/679. Această sancțiune a fost însoțită de măsura corectivă, constând în implementarea de măsuri tehnice și organizatorice adecvate, inclusiv prin instalarea de sisteme de operare cu suport activ din partea producătorului, soluții antivirus complete și actualizate pe toate echipamentele IT din rețeaua operatorului, respectiv securizarea accesului extern, după caz, la echipamentele infrastructurii operatorului.

## 10. FIȘĂ DE CAZ - Divulgarea și accesul neautorizat la datele cu caracter personal ale angajaților operatorilor din portofoliu

Un furnizor de servicii a notificat Autoritatea națională de supraveghere prin completarea formularului privind încălcarea securității datelor cu caracter personal conform Regulamentului (UE) 2016/679, cu privire la faptul că a fost ținta unui atac cibernetic, baza de date a acestuia fiind arhivată în format ZIP, criptată de mai multe ori și parolată.

Accesul neautorizat a fost realizat de la distanță pe unul dintre calculatoarele din rețea, al cărui utilizator avea și rolul de administrator de domeniu, existând elemente care indicau cunoașterea de către atacator a conturilor de administrare și a parolelor de acces asociate lor.

Au fost afectate datele cu caracter personal ale unui număr semnificativ de persoane fizice, respectiv: nume, prenume, CNP, domiciliu, funcție, salariu, sporuri și alte drepturi salariale. Furnizorul de servicii nu avea implementate anterior producerii incidentului proceduri privind crearea, complexitatea și schimbarea parolelor de acces, precum și modalitatea autentificării suplimentare. Furnizorul de servicii avea serverul de backup conectat la serverul de producție, fapt care a permis accesul facil al atacatorului la copiile de siguranță ale acestuia ș,i ulterior, i-a permis ștergerea acestora.

În urma investigației efectuate de Autoritatea națională de supraveghere, s-a constatat că furnizorul de servicii a încălcat prevederile art. 32 alin. (1) și art. 32 alin. (2) din Regulamentul (UE) 2016/679, deoarece nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată și accesul neautorizat la datele cu caracter personal transmise, stocate și prelucrate într-un alt mod, astfel cum avea obligația conform art. 5 alin. (1) lit. f) din Regulamentul (UE) 2016/679.

Aceasta a condus la divulgarea și accesul neautorizat la datele cu caracter personal ale unor salariați ai clienților din portofoliu (nume, prenume, CNP, domiciliu, funcție, salariu, sporuri și alte drepturi salariale).

Autoritatea națională de supraveghere a sancționat furnizorul de servicii cu amendă în cuantum de 24.887 lei, echivalentul sumei de 5.000 de euro, pentru încălcarea prevederilor art. 32 alin. (1) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

Totodată, s-au dispus operatorului măsuri corective constând în verificarea periodică a respectării procedurilor de lucru implementate referitoare la protecția datelor cu caracter personal, precum și instruirea periodică a persoanelor care acționează sub autoritatea sa, inclusiv cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal.

**11. FIȘĂ DE CAZ - Divulgarea și accesul neautorizat la datele cu caracter personal în urma unui atac cibernetic**

Un operator a notificat Autoritatea națională de supraveghere prin completarea formularului privind încălcarea securității datelor cu caracter personal conform Regulamentului (UE) 2016/679, cu privire la faptul că a fost victima unui atac informatic ransomware Lynx, inițiat printr-un acces neautorizat în infrastructura informatică, printr-o conexiune VPN. Atacatorul a generat atât criptarea și restricționarea accesului la baza de date a operatorului, cât și imposibilitatea funcționării sistemului informatic.

În urma investigației efectuate de Autoritatea națională de supraveghere s-a constatat că operatorul a încălcat prevederile art. 32 alin. (1) lit. b) și d) și art. 32 alin. (2) din Regulamentul (UE) 2016/679, deoarece nu a pus în aplicare măsuri tehnice și organizatorice adecvate și nu a realizat testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării, destinate să pună în aplicare în mod eficient principiile de protecție a datelor și să integreze garanțiile necesare în cadrul prelucrării.

Aceasta a condus la divulgarea și accesul neautorizat la datele cu caracter personal (date de identificare angajați, date financiare angajați, privitoare la salariile încasate, date bancare angajați, respectiv conturile bancare ale acestora, conturi bancare ale clienților/colaboratorilor din care s-a încasat contravaloarea produselor comercializate de operator) ale unui număr semnificativ de persoane fizice vizate, în urma unui atac de tip ransomware, care a avut ca vulnerabilitate credențialele de utilizator legitim/activ, atacatorul reușind să cripteze întreaga infrastructură informatică a operatorului.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 40.663 lei, echivalentul a 8.000 euro, pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și d) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

Totodată, în temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, s-au dispus următoarele măsuri corective:

- implementarea autentificării multifactoriale pentru toate conturile de utilizator/administrator care se pot conecta de la distanță în infrastructura IT a operatorului
- implementarea tehnică și organizatorică a unei politici de complexitate a parolelor utilizate pentru conturile respective.

## 12. FIȘĂ DE CAZ - Divulgarea și accesul neautorizat la date personale

Un operator a notificat Autoritatea națională de supraveghere prin completarea formularului privind încălcarea securității datelor cu caracter personal conform Regulamentului (UE) 2016/679, cu privire la faptul că a fost victima unui atac informatic în urma căruia au fost afectate date cu caracter personal, aflate pe serverul de e-mail și website-ul operatorului, respectiv datele din cărțile de identitate deținute în copie, adrese de e-mail, numere de telefon.

În urma investigației efectuate de Autoritatea națională de supraveghere, s-a constatat că operatorul a încălcat prevederile art. 32 alin. (1) lit. b) și d) și art. 32 alin. (2) din Regulamentul (UE) 2016/679, deoarece nu a pus în aplicare măsuri tehnice și organizatorice adecvate și nu a realizat testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice.

Aceasta a condus la divulgarea și accesarea neautorizată a datelor cu caracter personal din cărțile de identitate deținute în copie, adrese de e-mail, numere de telefon ale unor persoane vizate (clienți), în urma unui atac informatic, atacatorul reușind să acceseze bazele de date de pe serverul de e-mail și website-ul societății.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 10.162 lei, echivalentul a 2.000 de euro pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și d) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

## B. Investigații referitoare la prelucrarea datelor cu caracter personal de către autorități și instituții publice

În anul 2025, Autoritatea națională de supraveghere a efectuat investigații din oficiu privind prelucrarea datelor cu caracter personal de către autorități și instituții publice, precum instituții de învățământ din domeniul public.

Acestea s-au concentrat pe verificarea respectării dispozițiilor Regulamentului (UE) 2016/679, cu privire la desemnarea responsabilului cu protecția datelor (art. 37 – art. 39), precum și cu privire la asigurarea securității prelucrării, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau a deteriorării accidentale (art. 32 – art. 34), verificarea modalității de furnizare a informațiilor referitoare la prelucrarea datelor cu caracter personal, inclusiv a modalităților de exercitare a drepturilor persoanei vizate (art. 12 – 22 din Regulamentul (UE) 2016/679).

De asemenea, s-a avut în vedere și verificarea respectării prevederilor Legii nr. 190/2018.

Ca rezultat al investigațiilor, au fost aplicate operatorilor sancțiuni contravenționale și măsuri corective.

Măsurile corective dispuse au inclus revizuirea și actualizarea măsurilor tehnice și organizatorice, asigurarea conformității cu prevederile Regulamentului (UE) 2016/679, implementarea și actualizarea unor proceduri de notificare a încălcării securității datelor cu caracter personal care să cuprindă inclusiv modul de raportare și tratare a încălcărilor de securitate.

În majoritatea cazurilor, entitățile/operatorii au implementat măsurile corective dispuse, în termenul stabilit de Autoritatea națională de supraveghere.

În ceea ce privește sesizările primite împotriva autorităților și instituțiilor publice, prezentăm în continuare câteva **cazuri relevante**:

## 1. FIȘĂ DE CAZ - Atac cibernetic executat asupra infrastructurii informatice a unei primării

O primărie a notificat o încălcare a securității datelor cu caracter personal prin transmiterea unui formular privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679.

Autoritatea națională de supraveghere a constatat în cadrul investigației efectuate că operatorul nu a adoptat măsuri de securitate adecvate în vederea asigurării confidențialității datelor prelucrate, ceea ce a condus la încălcarea securității datelor cu caracter personal.

Incidentul a condus la divulgarea neautorizată a datelor cu caracter personal (nume, prenume, CNP, data nașterii) pentru un număr considerabil de persoane vizate, neprecizat de operator.

Operatorul a fost sancționat cu avertisment pentru încălcarea art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679, contravenție prevăzută de art. 14 alin. (2) lit. a) din Legea nr. 190/2018.

Sancțiunea a fost însoțit de măsura corectivă de a asigura conformitatea dispozițiilor prevăzute de art. 32 din Regulamentul (UE) 2016/679, în sensul implementării unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, inclusiv prin implementarea autentificării multifactoriale pentru toate conturile de utilizator/administrator care se pot conecta de la distanță în infrastructura IT a operatorului, respectiv implementarea tehnică și organizatorică a unei politici privind complexitatea parolelor utilizate pentru aceste conturi.

Operatorul a furnizat Autorității naționale de supraveghere dovezi cu privire la îndeplinirea măsurii corective dispuse.

**2. FIȘĂ DE CAZ – Divulgarea și accesul neautorizat la date prin intermediul unei platforme disponibile public**

Autoritatea națională de supraveghere a primit o petiție prin care a fost sesizată existența unei platforme online, accesibile public prin intermediul unui link, utilizată de o instituție publică pentru furnizarea unui serviciu destinat cetățenilor.

Platforma online permitea înregistrarea și consultarea unor sesizări aflate în competența de soluționare a instituției în cauză. În cadrul platformei respective au fost identificate sesizări care conțineau date cu caracter personal aparținând unor terți/persoane fizice.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat încălcarea prevederile art. 25 alin. (1) din Regulamentul (UE) 2016/679, art. 32 alin. (1) lit. a) și b) din Regulamentul (UE) 2016/679, întrucât operatorul nu a implementat suficiente măsuri de securitate, ceea ce a condus la pierderea confidențialității datelor cu caracter personal (transmise de către cetățeni prin depunerea sesizărilor pe platforma respectivă (de ex: nume, prenume, adresă, număr înmatriculare, etc.).

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea prevederilor art. 25 alin. (1) din Regulamentul (UE) 2016/679 și ale art. 32 alin. (1) lit. a) și b) din Regulamentul (UE) 2016/679.

De asemenea, s-a dispus măsura corectivă de implementare tehnică a unui mecanism de pseudonimizare a datelor cu caracter personal din corpul sesizărilor ce pot fi încărcate de cetățeni în platformă, astfel încât conținutul nemoderat al sesizării să nu poată fi vizualizat public, ci doar de către titularul sesizării, respectiv de către persoanele competente din cadrul operatorului.

Operatorul a implementat măsura corectivă dispusă de către Autoritatea națională de supraveghere.

**3. FIȘĂ DE CAZ – Divulgarea datelor cu caracter personal**

Autoritatea națională de supraveghere a fost sesizată cu privire la încălcarea prevederilor legale în materia prelucrării datelor cu caracter personal de către o instituție

publică din sistemul public de pensii, constând în publicarea pe site-ul instituției a datelor cu caracter personal ale unui număr semnificativ de pensionari cărora le-au fost alocate bilete de tratament.

Urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul a dezvăluit, în mod excesiv și fără temei legal, informații privind datele cu caracter personal ale mai multor beneficiari de bilete de tratament, constând în nume complet, CNP, adresă, număr de telefon, preferințe, punctaj individual, bază calcul, venituri, cu încălcarea prevederilor art. 5 alin. (1) lit. a), prin raportare la dispozițiile art. 6 alin. (1) din Regulamentul (UE) 2016/679, art. 5 alin. (1) lit. c) și art. 5 alin. (2) din același act normativ.

Pentru faptele constatate, Autoritatea națională de supraveghere a sancționat operatorul cu avertisment, însoțit de măsura corectivă constând în revizuirea procedurilor interne și instruirea personalului propriu, pentru ca, în toate situațiile, datele personale să fie prelucrate în conformitate cu principiile de prelucrare prevăzute la art. 5 din Regulamentul (UE) 2016/679 și în baza unui temei legal stabilit potrivit art. 6 din același regulament, astfel încât să nu fie prelucrate decât acele date personale care sunt necesare în vederea realizării scopurilor determinate stabilite potrivit atribuțiilor legale, prin implementarea unor garanții adecvate de protecție a datelor, precum aplicarea principiului reducerii la minimum a datelor, pseudonimizarea și criptarea acestora.

**4. FIȘĂ DE CAZ – Prelucrarea nelegală a datelor cu caracter personal prin accesarea și utilizarea înregistrărilor dintr-un sistem de supraveghere video**

Autoritatea națională de supraveghere a fost sesizată de către un sindicat cu privire la utilizarea imaginilor preluate din sistemul de supraveghere video al unui inspectorat județean de poliție în scopul cercetării disciplinare a polițiștilor.

Urmare a investigației efectuate, s-a reținut faptul că imaginile provenind din sistemul de supraveghere video al inspectoratului județean de poliție au fost accesate în baza dispoziției șefului inspectoratului și utilizate în faza prealabilă de cercetare din procedura disciplinară, deși sistemul de supraveghere video constituit din 20 de camere de supraveghere video fixe exterioare a fost instalat în scopul asigurării pazei și protecției persoanelor, bunurilor și valorilor acestora.

Autoritatea națională de supraveghere a constatat că operatorul a prelucrat ilegal datele personale a mai multor agenți de poliție (dintre care 14 au fost cercetați prealabil în cadrul procedurii disciplinare), prin accesarea și utilizarea înregistrărilor provenind din sistemul de supraveghere video al operatorului instalat în scopul "pazei obiectivelor, bunurilor, valorilor şi protecţiei persoanelor", într-un alt scop, incompatibil cu acesta, respectiv în scopul cercetării disciplinare a participanților la un protest, fiind încălcate prevederile art. 5 alin. (1) lit. a), b) și alin. (2) și art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Pentru faptele constatate, Autoritatea națională de supraveghere a sancționat operatorul cu avertisment, însoțit de măsura corectivă constând în reevaluarea necesității atingerii scopurilor propuse prin folosirea datelor provenite din sistemul de supraveghere video instalat la sediul operatorului, precum și evitarea folosirii sistemului de supraveghere video instalat în alte scopuri, incompatibile cu scopul inițial al prelucrării datelor.

## Secţiunea a 3-a: Activitatea de soluționare a plângerilor

### Prezentare generală

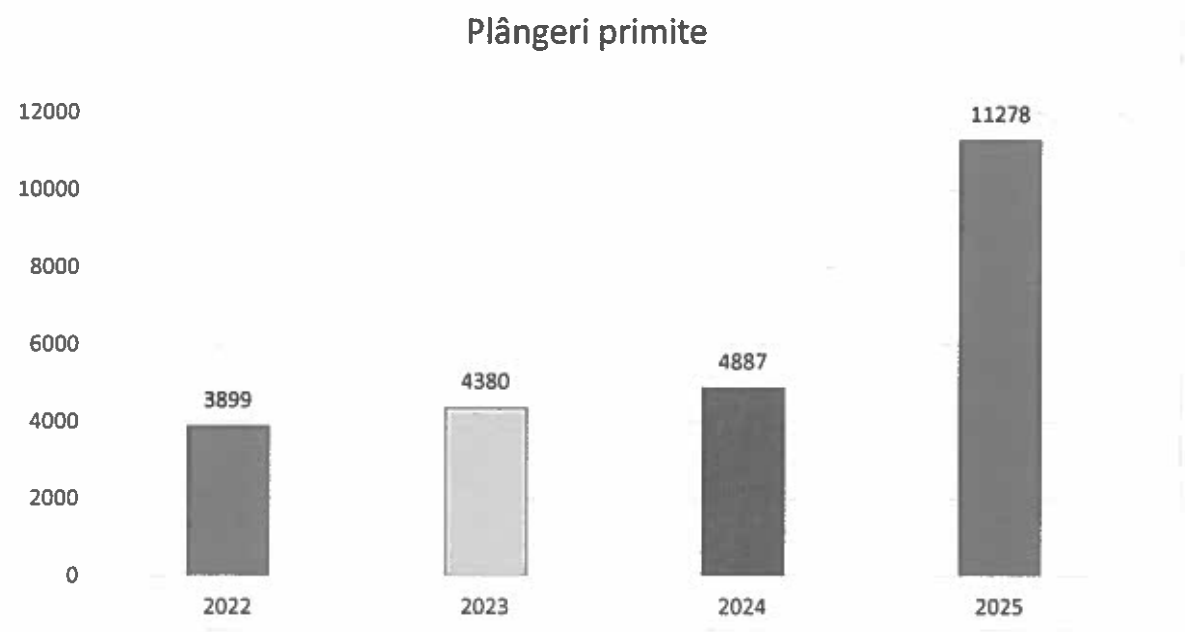
În cursul anului 2025, au fost primite **11.278 de plângeri** adresate Autorității naționale de supraveghere, ceea ce reprezintă o creștere semnificativă față de anii anteriori.

Aceste plângeri au vizat operațiuni de prelucrare a datelor cu caracter personal aflate sub incidența Regulamentului (UE) 2016/679, a Legii nr. 102/2005, republicată, a Legii nr. 190/2018, a dispozițiilor Legii nr. 506/2004 sau ale Legii nr. 363/2018.

Principalele aspecte rezultate în urma analizării plângerilor primite de Autoritatea națională de supraveghere au fost următoarele:

- prelucrarea datelor cu caracter personal cu nerespectarea principiilor legalității, echității și transparenței, precum și a condițiilor de legalitate prevăzute la art. 5 și 6 din Regulamentul (UE) 2016/679;

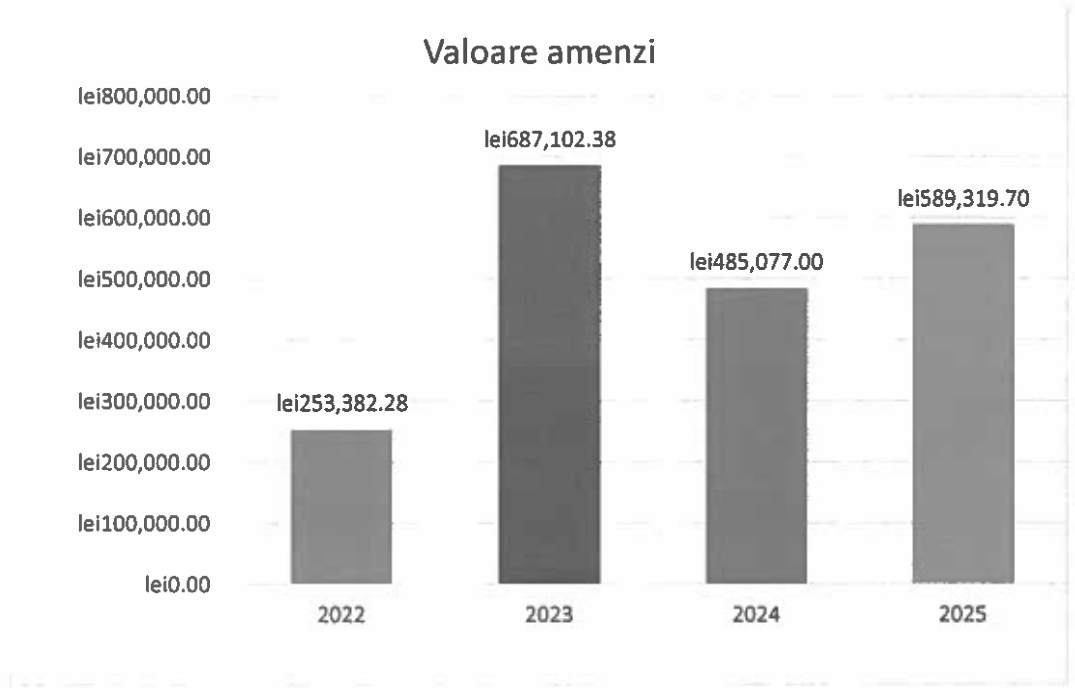
- încălcarea drepturilor persoanelor vizate, în special a dreptului de acces și a dreptului la ștergerea datelor, inclusiv în cadrul Sistemului de Informații Schengen (SIS);
- transmiterea de materiale și mesaje electorale către persoane fizice;
- blocarea sau restricționarea accesului la conturi de pe rețelele de socializare;
- divulgarea neautorizată a datelor cu caracter personal către terți, inclusiv prin intermediul rețelelor de socializare, al platformelor online, cât și la avizier;
- prelucrarea datelor cu caracter personal prin intermediul sistemelor de supraveghere video (în relațiile dintre persoane fizice, în condominii, precum și la locul de muncă);
- transmiterea de comunicări comerciale nesolicitate prin e-mail, telefon sau alte mijloace de comunicare;
- raportarea și prelucrarea datelor cu caracter personal în cadrul Biroului de Credit;
- prelucrarea datelor în domeniul jocurilor de noroc;
- încălcarea obligațiilor privind securitatea și confidențialitatea prelucrărilor de date cu caracter personal.




Pentru soluționarea plângerilor considerate admisibile au fost demarate **332 de investigații.**

Urmare a investigațiilor efectuate pe baza plângerilor, au fost aplicate următoarele **sancțiuni contravenționale**:

- ✓ 46 amenzi în baza Regulamentului (UE) 2016/679, reprezentând un cuantum total de 584.320 lei (echivalentul sumei de 116.500 euro);
- ✓ 1 amendă, în baza Legii nr. 506/2004, în cuantum de 5000 lei;
- ✓ 91 avertismente;
- ✓ 118 măsuri corective, în baza dispozițiilor art. 58 alin. (2) lit. a), c) și d) și e) din Regulamentul (UE) 2016/679;
- ✓ 1 decizie




**Măsurile corective** aplicate de Autoritatea națională de supraveghere au avut ca obiect principal următoarele:

• asigurarea conformității operațiunilor de prelucrare a datelor cu caracter personal cu dispozițiile Regulamentului (UE) 2016/679, prin implementarea măsurilor tehnice și organizatorice adecvate, inclusiv prin revizuirea bazelor de date și a aplicațiilor informatice utilizate, precum și prin instruirea corespunzătoare a personalului desemnat, astfel încât activitățile de marketing direct realizate prin servicii de comunicații electronice destinate publicului (telefon, SMS, e-mail) să se desfășoare cu respectarea strictă a prevederilor

Regulamentului (UE) 2016/679 și ale Legii nr. 506/2004, în special în ceea ce privește temeiul legal, exercitarea dreptului de opoziție, informarea completă a persoanelor vizate și respectarea principiilor de transparență prevăzute de art. 12–14 din Regulamentul (UE) 2016/679;

• implementarea unor proceduri interne eficiente pentru gestionarea, analizarea și soluționarea, în mod corect și în termenele legale, a cererilor formulate de persoanele vizate în exercitarea drepturilor prevăzute de Regulamentul (UE) 2016/679;

• asigurarea capacității operaționale a operatorului de a primi, evalua și soluționa toate cererile privind exercitarea drepturilor persoanelor vizate, prin adoptarea măsurilor tehnice și organizatorice necesare și prin instruirea adecvată a personalului implicat, astfel încât răspunsurile transmise să respecte cerințele de claritate, transparență și inteligibilitate prevăzute de art. 12–23 din Regulamentul (UE) 2016/679;

• asigurarea aplicării efective și fără întârzieri nejustificate a măsurilor de rectificare sau ștergere a datelor cu caracter personal, inclusiv în cazul conturilor deschise pe platformele operatorilor, precum și notificarea destinatarilor datelor, în conformitate cu art. 16, 17 și 19 din Regulamentul (UE) 2016/679 și cu respectarea principiului exactității prevăzut de art. 5 alin. (1) lit. d) din Regulamentul (UE) 2016/679;

• transmiterea unui răspuns complet și adecvat la cererile de exercitare a dreptului de acces, inclusiv prin furnizarea unei copii a datelor cu caracter personal prelucrate (cum ar fi înregistrările vocale), în conformitate cu dispozițiile art. 15 alin. (1), (3) și (4) din Regulamentul (UE) 2016/679, prin mijloace securizate de comunicare;

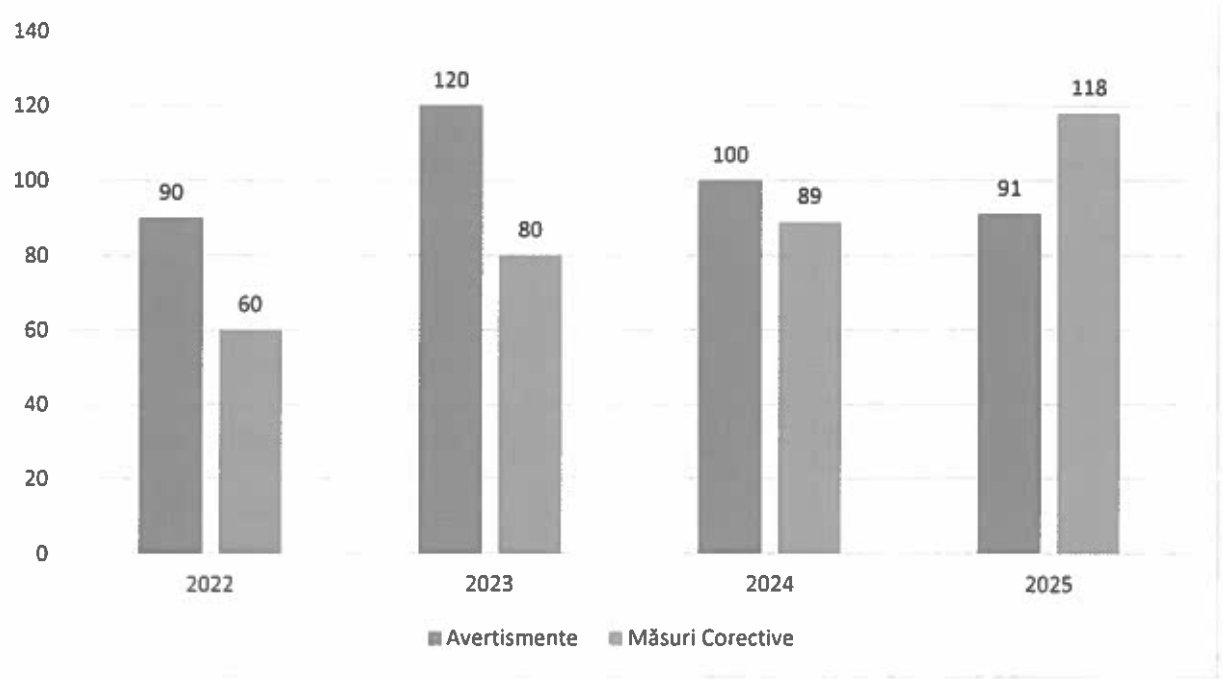
• asigurarea conformității operațiunilor de supraveghere video, inclusiv prin reorientarea camerelor instalate în exteriorul clădirilor astfel încât acestea să surprindă exclusiv perimetrul operatorului, fără a capta imagini din domeniul public;

• încetarea utilizării sistemelor de supraveghere video instalate în spații precum birouri, depozite sau hale de producție, în lipsa unui temei legal valabil pentru prelucrarea datelor cu caracter personal, în conformitate cu art. 6 din Regulamentul (UE) 2016/679;

• implementarea unei politici interne adecvate privind securitatea datelor, care să permită identificarea și evaluarea riscurilor, precum și notificarea Autorității naționale de supraveghere în cazul producerii unei încălcări a securității datelor cu caracter personal, în condițiile art. 33 alin. (1) din Regulamentul (UE) 2016/679, inclusiv prin instruirea

corespunzătoare a persoanelor care prelucrează date sub autoritatea sau în numele operatorului;

• stabilirea unor proceduri clare și riguroase pentru monitorizarea și actualizarea datelor transmise către terți (de exemplu, Biroul de Credit), în vederea prevenirii raportării unor date inexacte, incomplete sau neactualizate.




## 1. Principalele constatări rezultate din activitatea de soluționare a plângerilor

### A. Prelucrarea datelor cu caracter personal de către autoritățile publice

În anul 2025, Autoritatea națională de supraveghere a efectuat investigații ca urmare a unor plângeri care au vizat prelucrări de date cu caracter personal realizate de către autorități și instituții publice, în exercitarea atribuțiilor acestora.

Investigațiile efectuate au evidențiat situații în care operatorii nu au respectat principiile de prelucrare a datelor cu caracter personal, în special principiul legalității, al echității și al transparenței, precum și principiul reducerii la minimum a datelor, prevăzute de Regulamentul (UE) 2016/679.

În mai multe situații s-a constatat divulgarea neautorizată a datelor personale către terți, inclusiv către alte instituții publice sau către persoane fizice, fără existența unui temei legal care să justifice această prelucrare.

De asemenea, au fost identificate cazuri în care operatorii nu au implementat proceduri interne adecvate pentru protejarea datelor personale sau nu au respectat cerințele privind informarea persoanelor vizate și limitarea prelucrării datelor la ceea ce este necesar pentru îndeplinirea scopurilor declarate.

Potrivit art. 13 alin. (1) din Legea nr. 190/2018, "În cazul constatării încălcării prevederilor Regulamentului general privind protecţia datelor şi ale prezentei legi de către autorităţile/organismele publice, Autoritatea naţională de supraveghere încheie un proces-verbal de constatare şi sancţionare a contravenţiei prin care se aplică sancţiunea avertismentului şi la care anexează un plan de remediere".

**1. FIȘĂ DE CAZ**

O petentă a sesizat Autoritatea națională de supraveghere cu privire la o posibilă dezvăluire nelegală a datelor sale cu caracter personal de către o unitate administrativ-teritorială, reprezentată prin primar, către angajatorul petentei.

În fapt, petenta a formulat, în nume propriu, mai multe cereri adresate operatorului, în temeiul Legii nr. 544/2001 privind liberul acces la informațiile de interes public, referitoare la un imobil și un loc de înhumare din localitate, fără a menționa informații privind funcția sau locul său de muncă. Ulterior, nemulțumită de modul de soluționare a solicitărilor, aceasta a formulat și o reclamație administrativă prin care a solicitat cercetarea disciplinară a unor funcționari publici din cadrul primăriei.

Cererile petentei au fost semnate electronic, iar din certificatul calificat aferent semnăturii electronice rezulta faptul că acesta fusese emis de către o autoritate publică. În acest context, operatorul s-a adresat angajatorului petentei, solicitând cercetarea disciplinară a acesteia pentru modul de utilizare a semnăturii electronice.

În adresa transmisă angajatorului au fost dezvăluite datele personale ale petentei, respectiv numele și prenumele, adresa de domiciliu, funcția și locul de muncă, precum și informații privind petițiile depuse de aceasta în nume propriu și utilizarea semnăturii electronice. Potrivit susținerilor petentei, demersul operatorului nu a condus la aplicarea unei sancțiuni disciplinare.

În cadrul investigației, operatorul a susținut că datele privind funcția și locul de muncă ale petentei ar fi fost colectate din surse publice, respectiv din profilul de Facebook al acesteia și din apariții în mediul online.

Autoritatea națională de supraveghere a constatat că operatorul nu a făcut dovada existenței unui temei legal și al unui scop determinat, explicit și legitim pentru colectarea și prelucrarea datelor personale ale petentei, în special a celor privind funcția și locul de muncă, precum și pentru dezvăluirea către angajator a informațiilor referitoare la petițiile formulate de aceasta în nume propriu. Astfel, au fost încălcate principiile prelucrării datelor prevăzute de art. 5 alin. (1) lit. a), b), c) și alin. (2) din Regulamentul (UE) 2016/679, precum și condițiile de legalitate a prelucrării prevăzute de art. 6 din același regulament.

Totodată, s-a constatat că operatorul nu a făcut dovada informării petentei cu privire la colectarea suplimentară a datelor sale personale și la prelucrarea ulterioară a acestora, inclusiv dezvăluirea către angajator, fiind încălcate dispozițiile art. 12, art. 13 și art. 14 din Regulamentul (UE) 2016/679.

Față de cele constatate, s-a dispus sancționarea operatorului cu avertisment, în temeiul art. 13 din Legea nr. 190/2018.

Prin planul de remediere, Autoritatea națională de supraveghere a dispus operatorului următoarele măsuri corective:

1. revizuirea procedurilor interne, astfel încât să fie evitate colectarea și prelucrarea datelor personale ale persoanelor vizate cu încălcarea principiilor prevăzute de art. 5 și a condițiilor de legalitate stabilite de art. 6, art. 9 și art. 10 din Regulamentul (UE) 2016/679, precum și instruirea corespunzătoare a personalului care prelucrează date sub autoritatea operatorului, cu implicarea responsabilului cu protecția datelor;
2. asigurarea informării complete și corecte a persoanelor vizate cu privire la activitățile de prelucrare a datelor personale, prin furnizarea informațiilor prevăzute de art. 13 și/sau art. 14 din Regulamentul (UE) 2016/679, cu respectarea cerințelor de transparență prevăzute de art. 12 din același regulament, inclusiv prin publicarea acestora pe site-ul instituției și la sediul operatorului.

Ca urmare a demersurilor Autorității naționale de supraveghere, operatorul investigat a dat curs măsurilor corective dispuse.

**2. FIȘĂ DE CAZ**

O petentă a transmis Autorității naționale de supraveghere o plângere cu privire la o posibilă dezvăluire nelegală a datelor sale cu caracter personal de către o unitate administrativ-teritorială, reprezentată prin primar, în contextul comunicării unui document informativ către locuitorii comunei.

Petenta a reclamat faptul că operatorul a dezvăluit datele sale personale (nume, prenume și adresă) către mai multe persoane, prin intermediul unor notificări transmise locuitorilor comunei, prin care aceștia erau înștiințați cu privire la suspendarea alimentării cu apă.

În urma investigației efectuate, s-a constatat că operatorul a transmis notificări individuale către aproximativ 30 de persoane, respectiv proprietari ai imobilelor care utilizau rețeaua de apă, prin care aceștia erau informați despre suspendarea alimentării cu apă în comună. În conținutul acestor notificări au fost incluse datele personale ale petentei (nume, prenume și adresă).

În cadrul investigației, operatorul a susținut că menționarea datelor personale ale petentei în notificările respective a avut loc în contextul implementării unei măsuri administrative de interes local.

Autoritatea națională de supraveghere a constatat că operatorul nu a făcut dovada existenței unui temei legal care să justifice includerea datelor personale ale petentei în notificările distribuite către locuitorii comunei, în conformitate cu dispozițiile art. 6 din Regulamentul (UE) 2016/679.

De asemenea, s-a reținut că operatorul avea obligația de a respecta principiile prelucrării datelor cu caracter personal, inclusiv principiile legalității, legitimității și reducerii la minimum a datelor, prevăzute de art. 5 alin. (1) lit. a) și c), precum și obligația de responsabilitate prevăzută de art. 5 alin. (2) din Regulamentul (UE) 2016/679.

În acest context, s-a constatat că operatorul a încălcat prevederile art. 5 alin. (1) lit. a) și alin. (2), coroborat cu art. 6 din Regulamentul (UE) 2016/679, prin dezvăluirea nejustificată a datelor personale ale petentei către mai multe persoane.

Față de cele constatate, s-a dispus sancționarea operatorului cu avertisment pentru încălcarea dispozițiilor art. 5 alin. (1) lit. a) și alin. (2), coroborat cu art. 6 din Regulamentul (UE) 2016/679.

Totodată, prin planul de remediere Autoritatea națională de supraveghere a dispus operatorului următoarele măsuri corective:

1. revizuirea procedurilor interne privind prelucrarea datelor cu caracter personal;
2. instruirea periodică a persoanelor care prelucrează date sub autoritatea operatorului, astfel încât prelucrarea datelor personale să se realizeze cu respectarea principiilor și condițiilor prevăzute de art. 5 și art. 6 din Regulamentul (UE) 2016/679, evitându-se astfel dezvăluirea ilegală sau neautorizată a datelor.

Ca urmare a demersurilor Autorității naționale de supraveghere, operatorul investigat a dat curs măsurilor corective dispuse.

### 3. FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la o posibilă dezvăluire nelegală a datelor sale cu caracter personal de către un inspectorat de poliție județean către o altă autoritate publică, respectiv poliția locală.

Petentul a reclamat că a efectuat un apel la numărul unic de urgență 112, prin care a sesizat o încălcare a legislației privind deranjarea liniștii publice. La scurt timp după efectuarea apelului, acesta a fost contactat telefonic de către o persoană care s-a prezentat drept agent constatator, aceasta cunoscând datele sale cu caracter personal, faptul că apelase numărul 112, obiectul sesizării și alte detalii comunicate în cadrul apelului.

Ulterior, petentul s-a adresat mai multor instituții pentru clarificarea situației, iar inspectoratul de poliție județean i-a comunicat că transmiterea datelor sale către poliția locală s-a realizat în mod eronat.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul a transmis către polițiști locali datele de identificare ale petentului (nume, prenume, adresă și număr de telefon), colectate în urma apelului la numărul unic de urgență 112, fără existența unui temei legal pentru această dezvăluire.

Astfel, Autoritatea națională de supraveghere a reținut că operatorul nu a respectat principiile aplicabile prelucrării datelor cu caracter personal de către autoritățile competente, prevăzute de art. 5 alin. (1) lit. a) și alin. (2) din Legea nr. 363/2018, potrivit cărora datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent față de persoana vizată.

Față de cele constatate, s-a dispus sancționarea operatorului conform prevederilor legale aplicabile, pentru încălcarea dispozițiilor art. 5 alin. (1) lit. a) și alin. (2) din Legea nr. 363/2018.

Totodată, prin planul de remediere, Autoritatea națională de supraveghere a dispus operatorului măsuri corective constând în revizuirea procedurilor interne și instruirea personalului, astfel încât, în toate situațiile, datele cu caracter personal să fie prelucrate cu respectarea principiilor prevăzute de art. 5 din Legea nr. 363/2018.

Ca urmare a demersurilor instituției noastre, operatorul a luat măsurile necesare pentru implementarea planului de remediere dispus.

**4. FIȘĂ DE CAZ**

Autoritatea națională de supraveghere a fost sesizată de un petent, consilier local, cu privire la o posibilă prelucrare nelegală a datelor sale cu caracter personal de către o unitate administrativ-teritorială, reprezentată prin primar.

Petentul a reclamat faptul că a fost contactat telefonic de primarul comunei pentru a fi întrebat de ce nu s-a prezentat la o ședință a consiliului local, iar convorbirea telefonică a fost înregistrată fără a fi informat și fără a-și exprima consimțământul. Ulterior, înregistrarea convorbirii a fost prezentată în cadrul unei ședințe a consiliului local și a devenit disponibilă și pe internet.

În urma investigației efectuate, Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea dispozițiilor art. 5 alin. (1) lit. a) și art. 6 din Regulamentul (UE) 2016/679, referitoare la principiul legalității prelucrării datelor cu caracter personal.

Totodată, Autoritatea națională de supraveghere a dispus operatorului, prin planul de remediere, următoarele măsuri corective:

1. adoptarea sau revizuirea procedurilor interne și implementarea unor măsuri tehnice și organizatorice adecvate, inclusiv pentru asigurarea confidențialității datelor personale prelucrate, astfel încât operațiunile de prelucrare să fie conforme cu prevederile Regulamentului (UE) 2016/679 și să fie prevenite situații de dezvăluire ilegală sau neautorizată a datelor cu caracter personal;

2. instruirea periodică a persoanelor care prelucrează date cu caracter personal sub autoritatea operatorului.

De asemenea, în cadrul investigației s-a constatat că operatorul nu a făcut dovada desemnării unui responsabil cu protecția datelor, în conformitate cu prevederile art. 37 alin. (1) lit. a) din Regulamentul (UE) 2016/679, raportat la art. 10 din Legea nr. 190/2018, și nici a comunicării datelor de contact ale acestuia, conform art. 37 alin. (7) din același regulament.

Pentru aceste încălcări, operatorul a fost sancționat cu avertisment pentru nerespectarea dispozițiilor art. 37 alin. (1) lit. a) și art. 37 alin. (7) din Regulamentul (UE) 2016/679.

Totodată, Autoritatea națională de supraveghere a dispus măsura corectivă de a adopta măsurile necesare pentru asigurarea respectării prevederilor art. 37–39 din Regulamentul (UE) 2016/679, referitoare la desemnarea și funcționarea responsabilului cu protecția datelor.

Ca urmare a demersurilor Autorității naționale de supraveghere, operatorul a luat măsurile necesare pentru implementarea planului de remediere dispus.

## 5. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la o posibilă dezvăluire nelegală a datelor sale cu caracter personal de către fostul său angajator (autoritate publică).

Petentul a reclamat faptul că două adrese interne, întocmite de acesta în perioada în care era angajat al operatorului și care conțineau datele sale cu caracter personal, ar fi ajuns în posesia unui alt angajat al instituției. Potrivit susținerilor petentului, respectivele documente ar fi fost ulterior transmise de acest angajat către actualul angajator al petentului.

În cursul investigației s-a constatat că cele două adrese interne conțineau date cu caracter personal aparținând mai multor angajați, respectiv numele, prenumele și semnăturile olografe ale acestora, iar în cazul petentului era menționată și funcția ocupată.

De asemenea, s-a reținut că operatorul nu a putut demonstra temeiul legal în baza căruia un angajat al său a intrat în posesia acestor documente interne, înregistrate în cadrul unor compartimente ale instituției, și nici faptul că acesta ar fi avut atribuții care să justifice

accesul la respectivele documente. Astfel, datele cu caracter personal ale petentului și ale altor angajați au fost dezvăluite unei persoane care nu era autorizată să le prelucreze.

Autoritatea națională de supraveghere a avut în vedere faptul că, potrivit art. 29 din Regulamentul (UE) 2016/679, orice persoană care acționează sub autoritatea operatorului și are acces la date cu caracter personal le poate prelucra doar la instrucțiunile operatorului, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede altfel. Totodată, în sensul regulamentului, are calitatea de „parte terță" orice persoană fizică sau juridică, alta decât persoana vizată, operatorul, persoana împuternicită de operator sau persoanele autorizate să prelucreze date sub autoritatea acestora.

În urma investigației, s-a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate de securitate, care să asigure că numai persoanele autorizate au acces la datele cu caracter personal prelucrate, fiind astfel încălcate prevederile art. 32 alin. (1), (2) și (4) din Regulamentul (UE) 2016/679.

Față de cele constatate, s-a dispus sancționarea operatorului cu avertisment pentru încălcarea dispozițiilor art. 32 alin. (1), (2) și (4) din Regulamentul (UE) 2016/679.

Totodată, Autoritatea națională de supraveghere a dispus operatorului, prin planul de remediere, măsura corectivă de a asigura conformitatea operațiunilor de prelucrare a datelor cu caracter personal cu prevederile Regulamentului (UE) 2016/679, prin implementarea unor măsuri tehnice și organizatorice adecvate, inclusiv prin instruirea periodică a persoanelor care prelucrează date sub autoritatea operatorului, astfel încât prelucrarea datelor persoanelor vizate să fie realizată cu respectarea cerințelor legale privind protecția datelor.

Ca urmare a demersurilor Autorității naționale de supraveghere, operatorul investigat a dat curs măsurilor corective dispuse.

**B. Nerespectarea drepturilor persoanelor vizate**

Nerespectarea drepturilor persoanelor vizate a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere în anul 2025.

Demersurile întreprinse pentru soluționarea plângerilor au evidențiat o serie de situații în care operatorii nu au respectat drepturile persoanelor vizate prevăzute de articolele 12–23 din Regulamentul (UE) 2016/679.

Investigațiile efectuate au relevat deficiențe în modul de gestionare a cererilor prin care persoanele vizate solicită acces la datele personale, rectificarea acestora, ștergerea datelor sau exercitarea altor drepturi prevăzute de regulament.

În mai multe situații, operatorii nu au furnizat un răspuns complet și în termenul legal la cererile primite sau nu au comunicat copia datelor personale prelucrate, limitându-se la furnizarea unor informații generale privind categoriile de date prelucrate. De asemenea, au fost identificate cazuri în care operatorii au menținut date inexacte sau neactualizate în sistemele lor de evidență, afectând dreptul persoanelor vizate la rectificarea datelor.

Aceste situații evidențiază necesitatea implementării unor proceduri interne clare pentru gestionarea cererilor persoanelor vizate și pentru asigurarea respectării obligațiilor legale privind comunicarea răspunsurilor în termenul prevăzut de regulament.

**1. FIȘĂ DE CAZ**

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea unei plângeri prin care un petent a reclamat faptul că și-a exercitat dreptul de acces la datele sale cu caracter personal printr-o cerere transmisă prin e-mail către o autoritate publică, solicitând o copie a tuturor datelor personale deținute de această autoritate, însă a primit un răspuns pe care l-a considerat incomplet.

În cursul investigației efectuate, a rezultat că solicitarea petentului a fost redirecționată către o direcție generală regională a finanțelor publice, instituție publică cu personalitate juridică, care administra dosarul fiscal al petentului. Această instituție publică cu personalitate juridică are calitatea de operator de date cu caracter personal în raport cu prelucrarea datelor petentului.

În acest context, Autoritatea națională de supraveghere a constatat că, în răspunsul transmis petentului, operatorul (direcția generală regională a finanțelor publice) s-a limitat la enumerarea categoriilor de date cu caracter personal prelucrate, fără a indica datele personale efectiv prelucrate în cazul concret al petentului și fără a-i comunica o copie a datelor sale, astfel cum este prevăzut în art. 15 din Regulamentul (UE) 2016/679.

De asemenea, din documentele analizate în cadrul investigației a reieșit că operatorul nu a făcut dovada transmiterii unui răspuns către petent în termenul legal de 30 de zile de

la primirea cererii de exercitare a dreptului de acces, termen prevăzut de art. 12 alin. (3) din Regulamentul (UE) 2016/679.

Ca urmare a celor constatate, Autoritatea națională de supraveghere a dispus sancționarea operatorului cu avertisment, pentru încălcarea dispozițiilor art. 12 alin. (3), raportat la art. 15 alin. (1) și (3) din Regulamentul (UE) 2016/679, întrucât nu a transmis petentului, în termenul legal de o lună de la primirea cererii, un răspuns complet la solicitarea prin care acesta și-a exercitat dreptul de acces și a solicitat comunicarea copiei datelor sale cu caracter personal.

Totodată, a fost dispusă față de operator și măsura corectivă de a transmite petentului, prin e-mail și în mod securizat, un răspuns complet la cererea formulată, inclusiv prin comunicarea copiei datelor sale personale din bazele de date ale operatorului.

Ca urmare a demersurilor întreprinse de Autoritatea națională de supraveghere, operatorul investigat a dat curs măsurii dispuse.

### 3. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea unei plângeri prin care un petent a reclamat faptul că o companie de curierat i-a încălcat drepturile de acces și ștergere a datelor cu caracter personal. Petentul a solicitat operatorului copii ale unor documente, eventuale înregistrări ale unor apeluri sau mesaje de tip SMS, precum și explicații cu privire la mențiunea „persoană agresivă" asociată datelor sale și ștergerea acesteia, menționând că nu a primit niciun răspuns la cererea transmisă.

În cursul investigației s-a constatat că operatorul prelucra, în cazul petentului, următoarele date cu caracter personal: nume și prenume, adresă de domiciliu și de ridicare/livrare, cont IBAN, număr de telefon, adresă de e-mail, precum și mențiunea „persoană agresivă" asociată datelor sale, scopul prelucrării fiind livrarea expedițiilor poștale. Operatorul a precizat că nu efectuează înregistrări ale convorbirilor mobil–mobil, deoarece nu dispune de această posibilitate tehnică.

În ceea ce privește mențiunea „persoană agresivă", operatorul a susținut că aceasta nu reprezintă o dată cu caracter personal, fiind o notă introdusă într-un sistem informatic intern, fără o perioadă de stocare stabilită, și că persoana vizată ar putea solicita ștergerea acesteia prin intermediul departamentului de relații cu clienții.

Autoritatea națională de supraveghere a apreciat însă că această mențiune constituie dată cu caracter personal, în sensul art. 4 alin. (1) din Regulamentul (UE) 2016/679, deoarece se referă la o persoană identificabilă prin asocierea cu celelalte date existente în baza de date a operatorului. De asemenea, a fost avută în vedere jurisprudența Curții de Justiție a Uniunii Europene (Cauza C-434/16), potrivit căreia opiniile și evaluările referitoare la comportamentul sau aptitudinile unei persoane identificabile pot reprezenta date cu caracter personal.

Totodată, s-a reținut că, deși operatorul a invocat interesul său legitim de a evita situații de risc pentru angajații săi, acesta trebuie pus în balanță cu dreptul fundamental la viață privată al persoanei vizate, în special în contextul în care o astfel de mențiune ar putea fi introdusă în mod arbitrar, în urma unei conversații telefonice neînregistrate, și ar putea conduce la restricționarea accesului persoanei vizate la serviciile operatorului.

În acest context, Autoritatea națională de supraveghere a constatat că operatorul nu a prezentat un temei legal pentru prelucrarea acestei categorii de date și nici nu a șters mențiunea „persoană agresivă" ca urmare a cererii formulate de petent.

Ca urmare a constatărilor din cadrul investigației efectuate, operatorul a fost sancționat cu amendă în cuantum de 5.095 lei, echivalentul sumei de 1000 euro, pentru prelucrarea ilegală a datelor cu caracter personal ale petentului, respectiv a mențiunii „persoană agresivă", cu încălcarea principiilor prevăzute de art. 5 alin. (1) lit. a), c) și e), raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Totodată, în cadrul investigației s-a constatat că operatorul nu a comunicat petentului copia datelor personale prelucrate în cazul său, așa cum acesta solicitase prin cererea de acces. În plus, deși operatorul a susținut că a transmis un răspuns prin care a enumerat doar categoriile de date prelucrate, acesta nu a făcut dovada comunicării răspunsului în termenul prevăzut de art. 12 alin. (3) și (4) din Regulamentul (UE) 2016/679.

În consecință, operatorul a fost sancționat cu amendă în cuantum de 15.285 lei, echivalentul sumei de 3000 euro, pentru încălcarea dispozițiilor art. 12 alin. (3) și (4), raportat la prevederile art. 15 alin. (1) și (3) și art. 17 din Regulamentul (UE) 2016/679, întrucât nu a făcut dovada că a răspuns în termenul legal la cererea prin care petentul și-a exercitat dreptul de acces la date și dreptul de ștergere, cerere prin care a solicitat inclusiv o copie a documentelor ce conțin datele sale personale.

Totodată, Autoritatea națională de supraveghere a dispus față de operator următoarele măsuri corective:

1. transmiterea unui răspuns complet la cererea petentului, inclusiv prin comunicarea, în mod securizat, a copiei datelor sale personale din baza de date a operatorului, în conformitate cu art. 15 alin. (1), (3) și (4) din Regulamentul (UE) 2016/679;

2. reanalizarea necesității colectării și stocării mențiunii „persoană agresivă", inclusiv în cazul petentului, prin raportare la principiile prevăzute de art. 5 alin. (1) lit. a), c) și e) și la art. 6 alin. (1) din Regulamentul (UE) 2016/679;

3. asigurarea conformității operațiunilor de prelucrare a datelor cu caracter personal cu prevederile Regulamentului (UE) 2016/679, prin adoptarea măsurilor tehnice și organizatorice necesare, inclusiv prin instruirea corespunzătoare a personalului desemnat, astfel încât operatorul să poată analiza și soluționa în mod corect cererile prin care persoanele vizate își exercită drepturile, în termenele și condițiile prevăzute de art. 12-23 din regulament.

Operatorul a contestat procesul-verbal de constatare și sancționare, cauza aflându-se în prezent pe rolul instanțelor judecătorești.

**4. FIȘĂ DE CAZ**

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la o posibilă prelucrare nelegală a datelor sale cu caracter personal de către o instituție bancară, în contextul raportării unor informații financiare către Biroul de Credit.

Petentul a reclamat faptul că operatorul a transmis către Biroul de Credit date inexacte privind limita de credit aferentă unui produs financiar, aceasta fiind raportată cu valoarea „zero", deși limita reală de credit era de 7.600 lei. De asemenea, petentul a arătat că aceste informații eronate au fost menținute în evidențele Biroului de Credit pentru o perioadă de aproximativ cinci ani, în pofida solicitărilor repetate formulate în cursul anului 2025 pentru rectificarea datelor.

În cadrul investigației, Autoritatea națională de supraveghere a constatat că operatorul a menținut și a transmis către Biroul de Credit date inexacte referitoare la limita de credit a petentului și nu a asigurat actualizarea și corectarea acestora într-un termen rezonabil, deși persoana vizată a formulat în mod repetat cereri de rectificare.

Din analiza documentelor transmise de operator în cursul investigației a rezultat că, acesta a corectat datele inexacte ulterior declanșării investigației. Astfel, Autoritatea națională de supraveghere a constatat că operatorul nu a respectat obligația de a asigura exactitatea datelor prelucrate și dreptul persoanei vizate la rectificare, fiind încălcate prevederile art. 5 alin. (1) lit. d) și art. 16 din Regulamentul (UE) 2016/679.

În consecință, operatorul a fost sancționat contravențional cu amendă în cuantum de 15.163 lei, echivalentul sumei de 3.000 euro, pentru încălcarea art. 5 alin. (1) lit. d) și art. 16 din Regulamentul (UE) 2016/679.

Totodată, a fost dispusă măsura corectivă de asigurare a conformității operațiunilor de prelucrare a datelor cu caracter personal, prin stabilirea unor proceduri clare și riguroase pentru monitorizarea și actualizarea datelor raportate către terți, precum Biroul de Credit, astfel încât să fie evitată transmiterea unor date inexacte sau neactualizate.

Operatorul investigat a dat curs măsurii corective dispuse.

**5. FIȘĂ DE CAZ**

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la o posibilă prelucrare nelegală a datelor sale cu caracter personal de către angajatorul său, ca urmare a instalării unui sistem de supraveghere audio-video prin intermediul căruia angajații ar fi fost monitorizați în birouri, în zona de producție și în depozit, fără a fi informați în mod corespunzător.

Petentul a susținut că angajatorul nu a realizat informarea prealabilă obligatorie a angajaților, nu a consultat reprezentanții salariaților înainte de implementarea sistemului de monitorizare și nu a demonstrat că ar fi analizat sau utilizat mijloace mai puțin intruzive pentru atingerea scopului urmărit. De asemenea, petentul a arătat că nu a fost informat cu privire la durata de stocare a imaginilor rezultate din supravegherea video.

Totodată, petentul a reclamat că operatorul nu a răspuns cererilor prin care și-a exercitat dreptul de informare, de acces, de opoziție și de ștergere, și nici unei solicitări prin care a cerut o copie a înregistrărilor audio-video realizate de camera instalată în biroul contabil, indicând data și intervalul orar pentru care a solicitat înregistrarea.

În plus, petentul a semnalat instalarea unui filtru informatic care redirecționa automat toate mesajele de pe adresa de e-mail a unei angajate către o altă adresă de e-mail care nu aparținea societății, fapt ce ar fi permis transmiterea neautorizată a unor

documente ce conțineau date privind starea sa de sănătate (adeverință medicală, buletin de analize, raport medical, bilet de trimitere), situație ce ar fi constituit o posibilă încălcare a securității datelor.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul:

1. nu a făcut dovada consultării prealabile a angajaților sau a reprezentanților acestora, înainte de instalarea și punerea în funcțiune a sistemului de supraveghere video;

2. nu a demonstrat că a realizat informarea completă și explicită a angajaților și nici că alte metode mai puțin intruzive nu ar fi fost suficiente pentru atingerea scopului urmărit, astfel încât prelucrarea datelor nu a fost realizată în mod legal, echitabil și transparent;

3. nu a făcut dovada că a transmis petentului un răspuns în termenul legal de o lună la cererile prin care acesta și-a exercitat drepturile prevăzute de Regulamentul (UE) 2016/679;

4. nu a demonstrat că a adoptat măsuri tehnice și organizatorice adecvate pentru asigurarea confidențialității datelor personale, fiind posibilă redirecționarea neautorizată a mesajelor primite pe adresa de e-mail a unei angajate a operatorului, care conținea inclusiv date privind starea de sănătate a petentului, către o altă adresă de e-mail externă care nu aparținea operatorului

Față de cele constatate, operatorul a fost sancționat după cum urmează:

1. amendă în cuantum de 10.146 lei, echivalentul sumei de 2.000 euro, pentru încălcarea dispozițiilor art. 5 alin. (1) lit. a) și art. 6 din Regulamentul (UE) 2016/679, privind legalitatea prelucrării datelor;

2. amendă în cuantum de 5.073 lei, echivalentul sumei de 1.000 euro, pentru încălcarea dispozițiilor art. 12 alin. (3), art. 15, art. 17 și art. 21 din Regulamentul (UE) 2016/679, referitoare la exercitarea drepturilor persoanelor vizate;

3. avertisment pentru încălcarea dispozițiilor art. 32 alin. (1) din Regulamentul (UE) 2016/679, privind securitatea prelucrării datelor.

Totodată, Autoritatea națională de supraveghere a dispus următoarele măsuri corective:

1. adoptarea măsurilor necesare pentru asigurarea conformității cu Regulamentul (UE) 2016/679 a sistemelor de supraveghere video, inclusiv limitarea

înregistrării imaginilor la perimetrul societății și eliminarea camerelor instalate în birouri, depozit și hala de producție, în lipsa unui temei legal;

2. realizarea informării complete a tuturor persoanelor vizate cu privire la prelucrarea datelor, în conformitate cu art. 12-14 din Regulamentul (UE) 2016/679;

3. elaborarea unor proceduri interne privind soluționarea cererilor persoanelor vizate, precum și instruirea periodică a personalului;

4. implementarea unei politici interne pentru identificarea și gestionarea incidentelor de securitate și notificarea acestora către Autoritatea națională de supraveghere, conform art. 33 din Regulamentul (UE) 2016/679;

5. transmiterea unui răspuns petentului la cererile prin care acesta și-a exercitat drepturile.

Operatorul a contestat procesul-verbal de constatare și sancționare în instanță.

### C. Nerespectarea principiilor, a condițiilor de prelucrare și divulgarea neautorizată a datelor cu caracter personal

O parte semnificativă din investigațiile efectuate pentru soluționarea plângerilor adresate Autorității naționale de supraveghere în anul 2025 a avut ca obiect încălcarea principiilor de prelucrare și divulgarea neautorizată a datelor cu caracter personal.

Ca urmare a demersurilor întreprinse pentru soluționarea plângerilor considerate admisibile, s-a constat că, în mai multe cazuri, datele persoanelor vizate au fost divulgate fără consimțământul persoanelor vizate și fără un temei legal justificat, încălcând art. 5 și art. 6 din Regulamentul (UE) 2016/679.

Totodată, date cu caracter personal, precum: nume, prenume, CNP, adresă și număr de telefon, au fost dezvăluite către un număr larg de destinatari prin afișarea la avizier, transmiterea prin e-mail sau distribuirea pe grupuri de WhatsApp.

Autoritatea națională de supraveghere a constatat, de asemenea, faptul că operatorii nu au implementat măsuri tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal, încălcând astfel prevederile art. 32 din Regulamentul (UE) 2016/679. În mai multe cazuri, măsurile tehnice și organizatorice insuficiente au condus la accesul neautorizat sau divulgarea datelor către terți fără temei legal.

În același timp, au fost identificate situații în care operatorii au prelucrat date personale în lipsa unei analize adecvate a temeiului legal aplicabil sau au colectat și utilizat date care nu erau necesare pentru scopurile declarate ale prelucrării. Aceste practici au condus la încălcarea principiilor privind legalitatea, limitarea scopului și reducerea la minimum a datelor prevăzute de regulament.

**1. FIȘĂ DE CAZ**

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la o posibilă prelucrare nelegală a datelor sale cu caracter personal de către o instituție bancară, în contextul emiterii unei polițe de asigurare împotriva dezastrelor naturale aferente unui credit imobiliar.

Petentul a menționat că, deși contractul de credit încheiat cu banca fusese închis ca urmare a achitării integrale a sumelor datorate, datele sale cu caracter personal ar fi fost utilizate ulterior pentru emiterea unei noi polițe de asigurare împotriva dezastrelor naturale, fără acordul său.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat că emiterea eronată a poliței de asigurare a fost determinată de verificări interne realizate de bancă asupra portofoliului de garanții, în scopul identificării imobilelor pentru care polițele de asigurare expiraseră. Astfel, deoarece polița anterioară aferentă imobilului petentului depășise termenul de valabilitate, banca a transmis către societatea de asigurări solicitarea de emitere a unei noi polițe, fără a verifica dacă imobilul mai era adus în garanție la bancă și fără respectarea procedurii operaționale stabilite între bancă și societatea de asigurări.

De asemenea, a rezultat că banca a transmis către societatea de asigurări solicitări pentru emiterea unui număr ridicat de polițe, care au fost ulterior anulate, iar sumele aferente primelor de asigurare nu au fost debitate din conturile persoanelor vizate.

Față de cele constatate, operatorul a fost sancționat cu amendă în cuantum de 24.883 lei, echivalentul sumei de 5.000 euro, pentru încălcarea dispozițiilor art. 5 alin. (1) lit. a), raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679, întrucât a transmis către societatea de asigurări solicitarea de emitere a unui număr mare de polițe de asigurare

împotriva dezastrelor naturale, determinând astfel prelucrarea datelor cu caracter personal fără un temei legal valabil și cu încălcarea principiului legalității, echității și transparenței.

Totodată, instituția noastră a dispus operatorului și măsura corectivă de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de colectare și prelucrare ulterioară a datelor cu caracter personal, astfel încât să se evite utilizarea acestora cu încălcarea principiilor și condițiilor de legalitate. În acest sens, operatorul a fost obligat să aibă în vedere atât implementarea unor măsuri tehnice și organizatorice adecvate, inclusiv prin stabilirea unor proceduri interne scrise, cât și instruirea periodică a personalului care prelucrează date sub autoritatea sa.

Ca urmare a demersurilor Autorității naționale de supraveghere, operatorul investigat a dat curs măsurii corective dispuse.

**2. FIȘĂ DE CAZ**

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la o posibilă dezvăluire nelegală a datelor sale cu caracter personal de către angajatorul său, o instituție de învățământ superior, în contextul transmiterii unui mesaj pe adresa colectivă de e-mail a instituției.

Petentul a reclamat faptul că decanul facultății de psihologie, din cadrul universității unde acesta este profesor, a transmis pe adresa colectivă a universității un mesaj primit de la coordonatorul departamentului juridic, referitor la demersul juridic inițiat de petent împotriva angajatorului, ca urmare a sancționării sale pe care o considera abuzivă, în contextul calității sale de avertizor în interes public.

Mesajul respectiv a fost transmis întregului personal din subordinea decanului și includea mai multe documente (o adresă a instanței de judecată și copia cererii de chemare în judecată) care conțineau date cu caracter personal ale petentului (inclusiv adresa de domiciliu și codul numeric personal), precum și date referitoare la alte persoane.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul a dezvăluit datele cu caracter personal ale petentului fără consimțământul acestuia și fără existența unui alt temei legal pentru această prelucrare.

În consecință, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea dispozițiilor art. 5 alin. (1) lit. a) și lit. b) și art. 5 alin. (2), precum și ale art. 6 din Regulamentul (UE) 2016/679.

Totodată, Autoritatea națională de supraveghere a dispus operatorului și măsura corectivă de a asigura conformitatea operațiunilor de prelucrare a datelor personale cu prevederile Regulamentului (UE) 2016/679, inclusiv în ceea ce privește prelucrarea datelor angajaților, prin:

1. revizuirea procedurilor interne existente;
2. analizarea tuturor situațiilor de prelucrare a datelor pentru identificarea corectă a temeiului legal al prelucrării, în conformitate cu art. 6 din Regulamentul (UE) 2016/679;
3. instruirea corespunzătoare a persoanelor care prelucrează date sub autoritatea operatorului, astfel încât să fie evitată dezvăluirea ilegală sau neautorizată a datelor cu caracter personal ale persoanelor vizate.

Ca urmare a demersurilor Autorității naționale de supraveghere, operatorul investigat a dat curs măsurii dispuse.

### 3. FIȘĂ DE CAZ

Doi petenți au sesizat Autoritatea națională de supraveghere cu privire la o posibilă prelucrare nelegală a datelor lor cu caracter personal de către o agenție de turism. Aceștia au reclamat faptul că, pe contul de Facebook al agenției, a fost publicat un tabel care conținea date cu caracter personal aparținând unui număr mare de clienți, inclusiv ale petenților. Din dovezile transmise de aceștia a rezultat că în tabel erau dezvăluite informații precum: numele și prenumele clienților, ID-ul rezervării, hotelul sau locația rezervată și perioada sejurului.

Petenții s-au adresat, anterior, operatorului pentru a solicita explicații cu privire la dezvăluirea datelor lor personale, însă s-au declarat nemulțumiți de răspunsul primit.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate pentru asigurarea securității datelor, conform art. 32 din Regulamentul (UE) 2016/679. Această deficiență a condus la dezvăluirea neautorizată a datelor personale ale unui număr mare de persoane vizate pe pagina de Facebook a operatorului, în contextul organizării unei tombole pentru recompensarea clienților.

De asemenea, s-a constatat că operatorul nu a notificat Autoritatea națională de supraveghere cu privire la incidentul de securitate care a afectat datele personale ale unui număr mare de persoane vizate, prin dezvăluirea acestora pe pagina de Facebook, încălcând astfel dispozițiile și art. 33 din Regulamentul (UE) 2016/679.

În cadrul investigației operatorul nu a prezentat dovezi că a transmis petenților un răspuns complet la cererea prin care aceștia și-au exercitat dreptul de acces, în conformitate cu art. 15 din Regulamentul (UE) 2016/679, raportat la art. 12 alin. (3) și (4) din același regulament.

Pentru faptele constatate s-a dispus sancționarea operatorului cu:

1. amendă pentru încălcarea prevederilor art. 32 din Regulamentul (UE) 2016/679 în cuantum de 24.886 lei, echivalentul sumei de 5.000 euro;
2. amendă pentru încălcarea prevederilor art. 33 din Regulamentul (UE) 2016/679 în cuantum de 4.977 lei, echivalentul sumei de 1.000 euro;
3. avertisment, pentru încălcarea prevederilor art. 15 raportat la art. 12 alin. (3) si (4) din Regulamentul (UE) 2016/679.

Totodată, Autoritatea națională de supraveghere a dispus operatorului și trei măsuri corective constând în:

1. asigurarea conformității operațiunilor de prelucrare a datelor cu caracter personal cu Regulamentul (UE) 2016/679, prin implementarea unor măsuri tehnice și organizatorice adecvate specificului prelucrării și riscurilor identificate, inclusiv prin instruirea persoanelor care prelucrează date sub autoritatea operatorului și verificarea periodică a respectării instrucțiunilor transmise acestora;
2. adoptarea unor măsuri interne pentru detectarea rapidă, gestionarea și raportarea incidentelor de securitate, indiferent dacă acestea necesită sau nu notificarea autorității de supraveghere și/sau a persoanelor vizate, precum și instruirea periodică a personalului;
3. transmiterea către petenți a unui răspuns complet la cererea de exercitare a dreptului de acces.

Procesul-verbal de constatare și sancționare a fost contestat de operator în instanță.

## 4. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la o posibilă dezvăluire nelegală a datelor sale cu caracter personal de către un operator privat (o unitate de cazare), în contextul transmiterii unei facturi fiscale către o terță persoană.

Petentul a reclamat faptul că documentul contabil emis de operator, respectiv factura fiscală care conținea datele sale personale (nume, prenume, serie și număr CI), a fost transmis unei alte persoane fără acordul său.

În cadrul investigației operatorul a susținut că, la scurt timp după eliberarea camerei de către petent, o persoană a solicitat telefonic o copie a facturii fiscale, motivând că petentul ar fi pierdut documentul original. Operatorul a precizat că persoana respectivă a furnizat corect datele petentului, numele firmei beneficiare, data cazării și numărul camerei ocupate.

În urma acestei solicitări telefonice, un angajat al operatorului a transmis factura fiscală la o adresă de e-mail comunicată telefonic, operatorul motivând că are obligația de a emite un duplicat al facturii pentru ca societatea beneficiară să poată înregistra cheltuiala aferentă cazării în contabilitate.

Ca urmare a investigației efectuate s-a constatat că documentul contabil conținând datele cu caracter personal ale petentului (nume, prenume, serie și număr CI, precum și informații privind cazarea acestuia) a fost transmis unei terțe persoane, la o adresă de e-mail pentru care nu existau dovezi certe că aparține petentului sau societății comerciale indicate de acesta drept beneficiar.

Autoritatea națională de supraveghere a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura confidențialitatea datelor personale ale clienților, încălcând astfel dispozițiile art. 32 din Regulamentul (UE) 2016/679. Motivele invocate de operator pentru a justifica divulgarea datelor personale nu au fost reținute ca reprezentând un temei legal pentru această prelucrare.

Pentru faptele constatate, operatorul a fost sancționat cu amendă în cuantum de 9.954 lei, echivalentul sumei de 2.000 euro, pentru încălcarea dispozițiilor art. 32 alin. (1) lit. b) și d), alin. (2) și alin. (4) din Regulamentul (UE) 2016/679.

Totodată, instituția noastră a dispus operatorului măsura corectivă constând în elaborarea sau revizuirea procedurilor interne și instruirea periodică a tuturor persoanelor care prelucrează date sub autoritatea operatorului (angajați sau colaboratori), astfel încât să fie prevenită dezvăluirea ilegală sau neautorizată a datelor cu caracter personal ale clienților către terțe persoane.

Operatorul a contestat procesul-verbal de constatare și sancționare, cauza fiind pe rolul instanțelor de judecată.

**5. FIȘĂ DE CAZ**

Autoritatea națională de supraveghere a fost sesizată de o petentă cu privire la dezvăluirea datelor sale cu caracter personal pe rețeaua de socializare Facebook de către o angajată a unui operator furnizor local de utilități, aflat în subordinea unei unități administrativ-teritoriale.

Petenta a reclamat faptul că, în urma postării de către aceasta a unui comentariu referitor la programul de audiențe al primarului, o persoană care ocupa o funcție de conducere în cadrul operatorului a publicat un răspuns în care a dezvăluit informații personale privind situația juridică și financiară a petentei, respectiv existența unei presupuse restanțe la consumul de apă aferent unui imobil deținut de aceasta în coproprietate. Aceste informații erau accesibile angajatei operatorului în virtutea atribuțiilor sale de serviciu.

În urma analizei efectuate de responsabilul cu protecția datelor al operatorului s-a concluzionat că a avut loc un incident de securitate a datelor, în sensul art. 33 din Regulamentul (UE) 2016/679, constând în divulgarea neautorizată a datelor petentei pe Facebook. Incidentul a fost apreciat ca având un risc redus, întrucât au fost afectate date cu caracter general și pentru o perioadă scurtă de timp. Totodată, angajatului implicat i-a fost aplicată o sancțiune disciplinară constând în avertisment verbal.

Autoritatea națională de supraveghere a constatat, analizând documentele prezentate de operator în cadrul investigației derulate, că din acestea nu a rezultat cu claritate dacă, anterior producerii incidentului, personalul fusese instruit în mod adecvat cu privire la obligațiile ce îi revin în materia protecției datelor cu caracter personal, în special în ceea ce privește interdicția utilizării sau divulgării neautorizate a datelor la care au acces în exercitarea atribuțiilor de serviciu.

Față de cele constatate, operatorul a fost sancționat contravențional pentru încălcarea dispozițiilor art. 29 și art. 32 din Regulamentul (UE) 2016/679, cu amendă în cuantum de 5.084 lei, echivalentul sumei de 1.000 euro.

Totodată, Autoritatea națională de supraveghere a dispus operatorului și măsura corectivă de a asigura conformitatea operațiunilor de prelucrare a datelor cu caracter personal cu prevederile Regulamentul (UE) 2016/679, prin adoptarea unor măsuri tehnice și organizatorice adecvate, inclusiv prin instruirea periodică și corespunzătoare a persoanelor care au acces la date personale, astfel încât acestea să prelucreze datele exclusiv la cererea operatorului sau în temeiul obligațiilor legale, în conformitate cu art. 24, art. 29 și art. 32 din Regulamentul (UE) 2016/679, cu implicarea responsabilului cu protecția datelor.

Operatorul a transmis Autorității naționale de supraveghere informații privind modul în care s-a conformat măsurilor corective dispuse.

## D. Nerespectarea drepturilor persoanelor vizate în cadrul prelucrărilor transfrontaliere

Și în anul 2025, Autoritatea națională de supraveghere a continuat să fie implicată în derularea unor proceduri la nivelul Uniunii Europene privind soluționarea plângerilor referitoare la prelucrări de date cu caracter transfrontalier, în conformitate cu prevederile Regulamentului (UE) 2016/679, care reglementează cooperarea și asigurarea coerenței între autoritățile de supraveghere.

Investigațiile desfășurate în acest cadru au vizat clarificarea modului în care operatorii își îndeplinesc obligațiile prevăzute de Regulamentul (UE) 2016/679, inclusiv sub aspectul identificării sediului principal, al stabilirii competenței autorității de supraveghere și al cooperării dintre autoritățile implicate.

Autoritatea națională de supraveghere a fost consultată în calitate de autoritate vizată în situațiile în care prelucrările efectuate de operatori având sediul principal în alt stat membru al Uniunii Europene puteau produce efecte semnificative asupra persoanelor vizate din România sau implicau și un sediu stabilit pe teritoriul țării noastre.

În același timp, Autoritatea națională de supraveghere a transmis unele dintre plângerile primite către alte autorități de supraveghere principale ori a acționat ea însăși în această calitate, desfășurând investigații la nivelul operatorilor cu sediul principal în România, în vederea soluționării plângerilor care i-au fost transmise de către alte autorități de supraveghere din Uniunea Europeană, în urma aplicării mecanismelor de cooperare și coerență prevăzute de Regulamentul (UE) 2016/679.

În cadrul acestei secțiuni sunt prezentate câteva cazuri în care Autoritatea națională de supraveghere a finalizat demersurile de investigare în cooperare cu alte autorități de supraveghere, prin aplicarea de sancțiuni contravenționale și măsuri corective, fie în calitate de autoritate de supraveghere principală, în temeiul art. 60 din Regulamentul (UE) 2016/679, fie în calitate de autoritate competentă să soluționeze o plângere la nivel local, potrivit art. 56 din același regulament.

Acest capitol evidențiază situațiile în care prelucrarea datelor cu caracter personal a implicat elemente transfrontaliere, făcând necesară cooperarea dintre autoritățile de supraveghere din statele membre ale Uniunii Europene, în conformitate cu mecanismele de cooperare instituite de Regulamentul (UE) 2016/679.

### 1. FIȘA DE CAZ

În două cazuri similare, având ca obiect încălcarea dreptului de acces și a condițiilor de legalitate a prelucrării datelor cu caracter personal, Autoritatea națională de supraveghere a fost desemnată autoritate de supraveghere principală, în urma aplicării mecanismelor de cooperare și coerență prevăzute de Regulamentul (UE) 2016/679.

Plângerile au fost formulate de persoane vizate ale căror date cu caracter personal au fost colectate indirect de către un operator cu sediul în România, în scopul participării la sondaje de opinie, în schimbul obținerii unor recompense. Acestea au fost transmise de către autoritățile de supraveghere de reședință ale petenților și au fost soluționate de Autoritatea națională de supraveghere, în calitate de autoritate de supraveghere principală.

În fapt, petenții au reclamat primirea unor comunicări electronice care nu conțineau informațiile prevăzute de Regulamentul (UE) 2016/679 și, în acest context, și-au exercitat dreptul de acces pentru a obține informații privind sursa datelor.

Aceștia și-au exprimat nemulțumirea atât față de răspunsurile primite din partea operatorului, cât și față de faptul că au continuat să primească comunicări electronice, fără a-și fi exprimat consimțământul.

În urma investigației efectuate, prin procesul-verbal de constatare/sancționare, Autoritatea națională de supraveghere a reținut săvârșirea următoarele fapte:

1. încălcarea dispozițiilor art. 15 din Regulamentul (UE) 2016/679, coroborate cu art. 12 alin. (1) din același regulament, prin neîndeplinirea obligației de a furniza persoanelor vizate informațiile prevăzute de art. 15, inclusiv informații referitoare la sursa datelor, ca urmare a exercitării dreptului de acces;

2. încălcarea dispozițiilor art. 14 din Regulamentul (UE) 2016/679, raportate la art. 12 alin. (1), prin neinformarea completă a persoanelor vizate cu privire la prelucrarea datelor colectate de la terți, în conformitate cu cerințele art. 14 alin. (1) și (2) din același act normativ;

3. încălcarea dispozițiilor art. 6 alin. (1) din Regulamentul (UE) 2016/679, întrucât operatorul nu a făcut dovada existenței unui temei legal valabil pentru prelucrarea datelor cu caracter personal ale petenților, atât în ceea ce privește colectarea datelor în cadrul campaniei „Invită un prieten", cât și transmiterea de comunicări electronice prin care aceștia erau invitați să participe la sondaje de opinie sau la alte activități promoționale în schimbul unor recompense.

Având în vedere caracterul transfrontalier al prelucrării, au devenit aplicabile dispozițiile art. 60 din Regulamentul (UE) 2016/679, precum și cele ale art. 16 alin. (3)–(7) din Legea nr. 102/2005, republicată, referitoare la aplicarea sancțiunilor și a măsurilor corective prin decizie a președintelui Autorității naționale de supraveghere, care are la bază procesul-verbal de constatare și raportul personalului de control.

Prin decizie au fost dispuse următoarele sancțiuni și măsuri:

1. aplicarea unei amenzi contravenționale în cuantum de 24.886 lei, echivalentul sumei de 5.000 euro, pentru încălcarea dispozițiilor art. 15 din Regulamentul (UE) 2016/679, raportate la art. 12 alin. (1), în temeiul art. 83 alin. (5) lit. b) din același regulament;

2. aplicarea unei amenzi contravenționale în cuantum de 9.954 lei, echivalentul sumei de 2.000 euro, pentru încălcarea dispozițiilor art. 14 din Regulamentul (UE) 2016/679, raportate la art. 12 alin. (1), în temeiul art. 83 alin. (5) lit. a) din același act normativ;

3. aplicarea unei amenzi contravenționale în cuantum de 24.886 lei, echivalentul sumei de 5.000 euro, pentru încălcarea dispozițiilor art. 6 alin. (1) din Regulamentul (UE) 2016/679, în temeiul art. 83 alin. (5) lit. a) din regulament;

4. măsura corectivă prevăzută de art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, constând în instruirea periodică a personalului societății cu privire la soluționarea corectă a cererilor persoanelor vizate și la respectarea condițiilor de legalitate a prelucrării datelor cu caracter personal.

În cadrul investigației, operatorul a declarat că a exclus adresele de e-mail ale petenților din orice comunicări ulterioare, iar la momentul ștergerii conturilor acestora au fost eliminate și informațiile referitoare la sursa datelor. De asemenea, operatorul a precizat că a încetat desfășurarea campaniei respective, iar din baza de date au fost șterse toate adresele de e-mail ale persoanelor care nu au optat pentru inițierea unei relații contractuale.

Procesul-verbal de constatare și decizia Autorității naționale de supraveghere au fost contestate în fața instanțelor judecătorești.

## 2. FIȘA DE CAZ

În cursul anului 2025, Autoritatea națională de supraveghere a avut calitatea de autoritate de supraveghere principală în procedura de soluționare a unei plângeri formulate împotriva unei societăți care desfășoară activități în domeniul jocurilor de noroc, deoarece operatorul își are unicul sediu în România.

Plângerea a fost transmisă de autoritatea de supraveghere de reședință a petentului, care a invocat faptul că operatorul nu ar fi dat curs cererilor sale de exercitare a dreptului de acces cu privire la datele cu caracter personal prelucrate prin intermediul platformei pe care o deține. Prin cererile formulate, petentul a solicitat operatorului o serie de informații privind conturile sale de utilizator. Petentul a susținut că operatorul nu a transmis niciun răspuns la solicitările formulate.

În urma investigației efectuate de Autoritatea națională de supraveghere s-a constatat că solicitările petentului au fost transmise la o altă adresă de e-mail decât cea pusă la dispoziția persoanelor vizate pe toate website-urile administrate de către operator, respectiv adresa de contact a responsabilului cu protecția datelor (DPO). Ca urmare, cererile au fost direcționate către o adresă de e-mail incorectă, nefiind recepționate de operator și, implicit, neputând fi soluționate.

Totodată, ca urmare a verificărilor efectuate de departamentul competent al operatorului în bazele de date interne nu s-a identificat niciun cont de joc asociat numelui petentului pe niciunul dintre website-urile gestionate de acesta. Operatorul a pus la dispoziția Autorității naționale de supraveghere capturi de ecran din sistemele sale interne, care reflectă rezultatele căutărilor realizate utilizând atât numele complet, cât și numele de familie al petentului, pentru fiecare platformă administrată.

Operatorul a precizat că, pentru crearea unui cont de utilizator, este obligatorie furnizarea unui identificator unic, respectiv codul numeric personal pentru cetățenii români sau numărul permisului de ședere pentru cetățenii străini. În consecință, o identificare completă și certă a unui utilizator în sistemele operatorului poate fi realizată exclusiv pe baza acestor date.

Autoritatea națională de supraveghere a comunicat autorității de supraveghere din țara de reședință a petentului rezultatul demersurilor efectuate, în vederea informării petentului.

### 3. FIȘA DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu o plângere prin care o petentă a reclamat modul de soluționare a cererii sale de exercitare a dreptului de acces la datele cu caracter personal aferente contului său deschis pe platformele unui operator de jocuri de noroc, inclusiv informațiile referitoare la cererile de autoexcludere formulate.

Având în vedere că operatorul este o societate cu sediul social declarat într-un alt stat membru al Uniunii Europene, Autoritatea națională de supraveghere a transmis inițial plângerea către autoritatea de protecție a datelor din acest stat, în temeiul art. 56 din Regulamentul (UE) 2016/679. Autoritatea de supraveghere din statul respectiv nu s-a

considerat însă autoritate de supraveghere principală în acest caz, apreciind că societatea este înregistrată în acel stat exclusiv în scopuri fiscale.

În aceste condiții, Autoritatea națională de supraveghere a continuat soluționarea plângerii ca fiind un caz național, având în vedere că, pentru desfășurarea activităților specifice jocurilor de noroc, operatorul deține un sediu declarat pe teritoriul României.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat încălcarea dispozițiilor privind dreptul de acces și a dispus sancționarea contravențională a operatorului cu amendă în cuantum de 76.333 lei, echivalentul sumei de 15.000 euro, întrucât acesta nu a făcut dovada transmiterii, în termenul legal, a unui răspuns scris complet și corespunzător la cererea prin care petenta și-a exercitat dreptul de acces, sancțiunea fiind aplicată în temeiul art. 83 alin. (5) lit. b) din Regulamentul (UE) 2016/679.

Totodată, în baza art. 58 alin. (2) lit. c) și d) din Regulamentul (UE) 2016/679, au fost dispuse două măsuri corective constând în obligarea operatorului:

- să comunice petentei toate informațiile solicitate în cadrul cererii de acces;
- să adopte măsurile tehnice și organizatorice necesare, inclusiv prin instruirea corespunzătoare a personalului desemnat și implicarea responsabilului cu protecția datelor, astfel încât să asigure analizarea, soluționarea corectă și comunicarea adecvată a cererilor persoanelor vizate, în termenele și în condițiile prevăzute de art. 12–23 din Regulamentul (UE) 2016/679.

Operatorul a formulat contestație împotriva sancțiunii aplicate, iar cauza se află pe rolul instanțelor judecătorești.

# CAPITOLUL IV

# ACTIVITATEA ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE

În plan extern, activitatea Autorității naționale de supraveghere în anul 2025 a fost marcată prin participarea, în format fizic sau în format videoconferință, la o serie de reuniuni ale organismelor Uniunii Europene sau ale Consiliului Europei în domeniul protecției datelor cu caracter personal, precum și prin implicarea în activitățile desfășurate în cadrul acestora.

## Comitetul european pentru protecția datelor

În anul 2025, Comitetul european pentru protecția datelor a adoptat **25** avize pe marginea proiectelor de decizii ale autorităților de supraveghere referitoare la regulile corporatiste obligatorii pentru operatori/persoane împuternicite de operatori și **4** avize pe marginea proiectelor de mecanisme de certificare, în conformitate cu art. 42 din Regulamentul (UE) 2016/679.

În același timp, Comitetul european pentru protecția datelor a adoptat și emis o serie de orientări cu privire la aplicarea Regulamentului (UE) 2016/679, recomandări, declarații, note de informare, dintre care evidențiem:

- Orientările 02/2024 privind articolul 48 din Regulamentul (UE) 2016/679 – al căror scop este de a clarifica raționamentul și obiectivul acestui articol, inclusiv interacțiunea sa cu celelalte dispoziții ale capitolului V din Regulamentul (UE) 2016/679, și de a oferi recomandări practice operatorilor și persoanelor împuternicite de operatori din UE care pot primi cereri din partea autorităților din țări terțe de a divulga sau transfera date cu caracter personal. Obiectivul principal al dispoziției este de a clarifica faptul că hotărârile judecătorești sau deciziile pronunțate de autoritățile unei țări terțe nu pot fi recunoscute sau executate în mod automat și direct într-un stat membru al UE, subliniind astfel suveranitatea juridică în raport cu legislația unei țări terțe. Ca regulă generală, recunoașterea și caracterul executoriu al hotărârilor judecătorești și deciziilor străine sunt asigurate prin acorduri internaționale aplicabile. Indiferent dacă există sau nu un acord internațional aplicabil, în cazul în care un operator sau o persoană împuternicită de operator din UE primește și răspunde unei cereri de date cu caracter personal din partea unei

autorități dintr-o țară terță, un astfel de flux de date reprezintă un transfer în temeiul Regulamentului (UE) 2016/679 și trebuie să respecte articolul 6 și dispozițiile capitolului V.

➢ Recomandările 01/2025 privind Codul mondial antidoping al WADA din 2027 – Codul mondial antidoping (denumit în continuare „codul") vizează armonizarea politicilor, normelor și reglementărilor antidoping la nivel internațional și este completat de opt standarde internaționale cu obiectivul de a promova coerența între programele antidoping care sunt puse în aplicare în principal prin intermediul organizațiilor naționale antidoping. Cele opt standarde internaționale se referă la următoarele aspecte: protecția datelor; educație; informații și investigații; laboratoare; gestionarea rezultatelor; testare; derogări privind utilizarea terapeutică; și conformitatea. Comitetul reamintește că normele codului și standardele aferente au fost transpuse de statele membre în ordinea lor juridică națională, în conformitate cu structura lor națională și cu organizarea sportului. În calitate de semnatare ale Convenției internaționale UNESCO împotriva dopajului în sport din 2005 și ale Convenției antidoping a Consiliului Europei, statele membre trebuie să respecte angajamentele care decurg din ratificarea acestor convenții. Comitetul reamintește că, atunci când statele membre adoptă măsuri naționale antidoping, care cuprind acte legislative, reglementări, politici sau practici administrative, pe baza principiilor codului, acestea trebuie să asigure că măsurile respective sunt în conformitate cu dreptul SEE, inclusiv cu Regulamentul (UE) 2016/679. Prin urmare, în cazul în care dispozițiile codului și ale standardelor sale internaționale nu sunt conforme cu Regulamentul (UE) 2016/679, statele membre nu le pot transpune ca atare în măsuri naționale antidoping fără a încălca obligațiile care le revin în temeiul legislației UE/SEE și, prin urmare, fără a afecta nivelul de protecție a persoanelor fizice din SEE în ceea ce privește datele lor cu caracter personal. Comitetul subliniază că, în punerea în aplicare a măsurilor naționale antidoping, organizațiilor naționale antidoping, în calitate de operatori, sunt responsabile de prelucrarea datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 și, în calitate de autorități administrative, trebuie să lase neaplicate, dacă este necesar, dispozițiile naționale antidoping respective care ar contraveni unor dispoziții ale Regulamentului (UE) 2016/679 care au efect direct. Prin urmare, atunci când pun în aplicare legislația, reglementările, politicile sau practicile administrative naționale antidoping, statele membre ar trebui să evalueze cu atenție dacă dispozițiile codului și ale standardelor sale internaționale care implică prelucrarea datelor cu caracter personal sunt compatibile cu

Regulamentul (UE) 2016/679, astfel încât să se evite, de asemenea, posibilele încălcări ale legislației SEE de către organizațiile naționale antidoping și orice expunere la acțiunile corective și la sancțiunile autorităților competente pentru protecția datelor.

➢ Avizul 07/2025 privind Proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal de către Organizația Europeană de Brevete

Comitetul a analizat cadrul juridic al Organizației Europene de Brevete în ceea ce privește accesul autorităților publice la datele cu caracter personal transferate din Uniune către organizație și utilizarea acestora. În acest sens, Comitetul subliniază că evaluarea accesului autorităților publice în cazul de față este distinctă de evaluarea care corespunde nivelului de protecție oferit de o țară terță. Scenariul specific al unei decizii privind protecția adecvată a datelor cu caracter personal de către o organizație internațională necesită revizuirea normelor care determină modul în care organizația respectivă tratează cererile de acces ale autorităților publice.

➢ Avizul 26/2025 privind proiectul de decizie de punere în aplicare al Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal de către Regatul Unit

Comitetul s-a axat pe evaluarea atât a aspectelor generale privind protecția datelor din proiectul de decizie, cât și a accesului autorităților publice la datele cu caracter personal transferate din SEE către Regatul Unit în scopul aplicării legii și al securității naționale, inclusiv a căilor de atac disponibile persoanelor fizice din SEE. Comitetul a evaluat, de asemenea, dacă garanțiile prevăzute în cadrul juridic din Regatul Unit sunt în vigoare și eficiente.

➢ Avizul 27/2025 privind proiectul de decizie de punere în aplicare al Comisiei Europene în temeiul Directivei (UE) 2016/680 privind protecția adecvată a datelor cu caracter personal de către Regatul Unit

Evaluarea Comitetului privind nivelul de protecție adecvat oferit de Regatul Unit s-a axat pe noile evoluții ale cadrului juridic și pe elementele evidențiate în decizia anterioară privind nivelul de protecție adecvat. Obiectivul acestui aviz a fost de a identifica aspecte specifice privind modificările și evoluțiile legislative de la data adoptării primei decizii privind nivelul de protecție adecvat, care pot afecta nivelul de protecție oferit de Regatul Unit.

➢ Avizul 28/2025 referitor la proiectul de decizie de punere în aplicare al Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal de către Brazilia

Comitetul s-a axat pe evaluarea atât a aspectelor generale privind protecția datelor din proiectul de decizie, cât și a accesului autorităților publice la datele cu caracter personal transferate din SEE în scopul aplicării legii și al securității naționale, inclusiv căile de atac disponibile persoanelor fizice din SEE. De asemenea, Comitetul a evaluat dacă garanțiile prevăzute în cadrul juridic din Brazilia sunt în vigoare și eficiente. Comitetul a luat act de faptul că cadrul juridic privind protecția datelor, în special *Legea generală privind protecția datelor* (LGPD) din Brazilia, împreună cu decretele prezidențiale și regulamentele obligatorii emise de Autoritatea pentru protecția datelor din Brazilia (Agencia Nacional de Proteção de Dados), stabilesc cerințe – inclusiv în ceea ce privește principiile, drepturile persoanelor vizate, transferurile, supravegherea și căile de atac – care sunt strâns aliniate cu Regulamentul (UE) 2016/679 și cu jurisprudența Curții de Justiție a Uniunii Europene.

➢ Avizul comun 01/2025 al CEPD-AEPD privind propunerea de regulament privind măsurile de simplificare pentru IMM-uri și întreprinderile cu capital mic (SMMC), în special obligația de păstrare a evidențelor în temeiul art. 30 alin. (5) din Regulamentul (UE) 2016/679

CEPD și AEPD susțin obiectivul general al propunerii de a reduce sarcina administrativă pentru IMM-uri și întreprinderile mici cu capitalizare medie, atâta timp cât urmărirea acestui obiectiv nu duce la reducerea protecției drepturilor fundamentale ale persoanelor fizice, în special a dreptului fundamental la protecția datelor cu caracter personal. În acest sens, CEPD și AEPD salută faptul că modificările propuse la Regulamentul (UE) 2016/679 pentru a simplifica și a clarifica obligația de a ține evidența a activităților de prelucrare sunt specifice și limitate și nu afectează principiile fundamentale și alte obligații prevăzute de Regulamentul (UE) 2016/679. CEPD și AEPD salută eforturile de clarificare și simplificare privind condițiile în care se aplică derogarea prevăzută la articolul 30 alineatul (5) din Regulamentul (UE) 2016/679, prin dispoziția conform căreia această derogare nu se aplică prelucrării care „este susceptibilă să genereze un risc ridicat". Pentru a evita orice neînțelegere, CEPD și AEPD propun colegiuitorilor să clarifice în considerente că o evidență a activităților de prelucrare ar fi obligatorie numai pentru acele activități de prelucrare „susceptibile să genereze un risc ridicat". În ceea ce privește obligația de păstrare a

evidenței prevăzută la articolul 30 din Regulamentul (UE) 2016/679, CEPD și AEPD subliniază că, pe lângă facilitarea demonstrării ex-post a conformității, evidențele activităților de prelucrare constituie un mijloc foarte util pentru a sprijini respectarea mai multor cerințe ale Regulamentului (UE) 2016/679. Prin urmare, CEPD și AEPD încurajează întreprinderile și organizațiile care au mai puțin de 750 de angajați și care nu efectuează activități de prelucrare cu risc mare să aleagă metodele cele mai adecvate pentru a sprijini în mod corespunzător respectarea obligațiilor Regulamentului (UE) 2016/679 și pentru a nu avea un impact negativ asupra drepturilor persoanelor vizate. În plus, CEPD și AEPD ar aprecia precizări suplimentare cu privire la motivul pentru care noul prag al întreprinderilor sau organizațiilor cu mai puțin de 750 de angajați ar fi adecvat pentru cazul concret al Regulamentului (UE) 2016/679. În ceea ce privește referirile la IMM-uri, întreprinderile mici cu capitalizare medie și organizații din textul propunerii, CEPD și AEPD recomandă colegiuitorilor ca în articolul 30 alineatul (5) modificat din Regulamentul (UE) 2016/679 să facă referire la definițiile nou-introduse ale IMM-urilor și întreprinderilor mici cu capitalizare medie. În plus, recomandă colegiuitorilor să clarifice într-un considerent că termenul „organizație" care intră sub incidența derogării propuse în temeiul articolului 30 alineatul (5) din Regulamentul (UE) 2016/679 nu include autoritățile și organismele publice.

**Reguli Corporatiste Obligatorii**

Un aspect important în ceea ce privește transferurile internaționale de date cu caracter personal este reprezentat de evaluarea și aprobarea cererilor de reguli corporatiste obligatorii transmise de companii multinaționale. De asemenea, Autoritatea națională de supraveghere are un rol consultativ în privința transferurilor de date, indiferent de temeiul legal al acestora.

Regulile corporative obligatorii (BCRs) au fost introduse ca răspuns la nevoia organizațiilor de a avea o abordare globală în ceea ce privește protecția datelor cu caracter personal, în situația în care multe organizații dețineau mai multe filiale/sucursale situate pe tot globul, transferând date cu caracter personal la scară largă. Includerea BCRs în Regulamentul (UE) 2016/679 consolidează în continuare utilizarea lor ca garanție adecvată pentru a legitima transferurile de date cu caracter personal în țări terțe.

În anul 2025, Autoritatea națională de supraveghere a primit și a analizat cereri de aprobare a BCRs transmise de 35 de companii multinaționale.

Totodată, Autoritatea națională de supraveghere a acționat în calitate de co-revizor la cererile de aprobare a BCRs transmise de 7 companii în această perioadă și a fost membru în echipa de redactare a opiniei CEPD cu privire la 6 seturi de reguli corporatiste obligatorii.

În calitate de autoritate principală și autoritate co-revizor, Autoritatea națională de supraveghere a formulat o serie de observații și recomandări dintre care evidențiem următoarele:

- stabilirea unei proceduri pentru situația în care cererile persoanelor vizate sunt primite de alte departamente/persoane, precum și a termenelor de redirecționare a respectivelor cereri,
- păstrarea unei evidențe a cererilor de exercitare a drepturilor de la persoanele vizate,
- păstrarea unei evidențe a plângerilor primite de la persoanele vizate și întocmirea de către responsabilul cu protecția datelor a unui raport referitor la plângerile primite, obiectul plângerilor, precum și rezultatul soluționării acestora,
- includerea de mențiuni referitoare la dreptul de a se opune în contextul prelucrării datelor cu caracter personal în scop de marketing direct, informarea persoanei vizate, în mod explicit, în legătură cu acest drept, posibilitatea de exercitare a dreptului de a se opune prin mijloace automate care utilizează specificații tehnice, în contextul utilizării serviciilor societății informaționale,
- includerea de mențiuni exprese cu privire la dreptul persoanei vizate de a depune o plângere la în situația în care nu primește un răspuns/nu este mulțumită de răspunsul primit de la operator,
- păstrarea unei evidențe actualizate a modificărilor aduse regulilor corporatiste obligatorii,
- menționarea principiilor legate de prelucrarea datelor cu caracter personal, utilizând formularea din Regulamentul (UE) 2016/679,
- includerea de mențiuni referitoare la excepțiile de la furnizarea de informații către persoana vizată atunci când datele nu au fost obținute de la aceasta,
- includerea tuturor scenariilor în care se aplică dreptul de ștergere prevăzut de art. 17 din Regulamentul (UE) 2016/679,

- specificarea în mod clar a modalității de păstrare a evidenței activităților de prelucrare, a informațiilor ce vor fi incluse în respectiva evidență etc., în conformitate cu art. 30 din Regulamentul (UE) 2016/679,
- independența responsabilului cu protecția datelor și raportarea către managementul superior.

Procedura de aprobare a BCRs s-a modificat de la un sistem de recunoaștere reciprocă în conformitate cu Directiva 95/46/CE la sistemul actual în care toate BCRs trebuie să fie prezentate Comitetului european pentru protecția datelor în vederea obținerii unui aviz în temeiul art. 64 din Regulamentul (UE) 2016/679.

Această procedură presupune că toate autoritățile de supraveghere au posibilitatea de a transmite observații pe marginea cererilor BCRs, ceea ce duce la o procedură de cooperare ceva mai lungă. Procedura va ajuta Comitetul european pentru protecția datelor la redactarea avizului său dacă toate chestiunile problematice sunt soluționate înainte de demararea procedurii prevăzute la art. 64 din Regulamentul (UE) 2016/679.

În anul 2025, Comitetul european pentru protecția datelor a emis 25 avize în temeiul art. 64 din Regulamentul (UE) 2016/679, referitoare la proiectele de decizie înaintate de autoritățile de supraveghere referitoare la regulile corporatiste obligatorii.

**Solicitări de asistență reciprocă prin intermediul sistemului IMI**

În contextul cooperării cu alte autorități de supraveghere din UE în vederea asigurării asistenței reciproce, au fost gestionate solicitări cu privire la aplicarea și respectarea Regulamentul (UE) 2016/679. Solicitările venite din partea autorităților de supraveghere din Cehia, Finlanda, Italia, Slovacia, Suedia au vizat aspecte referitoare la primirea și înregistrarea valabilă a plângerilor potrivit art. 77 din Regulamentul (UE) 2016/679, publicarea datelor de contact ale responsabilului cu protecția datelor și comunicarea acestora către Autoritatea națională de supraveghere, plângeri privind utilizarea datelor biometrice pentru verificarea la distanță a identității persoanei fizice de către instituții financiare, legislația privind prelucrarea datelor personale ale angajaților, aplicarea de amenzi în sectorul public, consultarea Autorității naționale de supraveghere în ceea ce privește instrumentul OECD 0487 „Declarație privind accesul guvernamental la datele cu caracter personal deținute de entitățile din sectorul privat".

**Contribuții din perspectiva protecției datelor cu caracter personal**

În cursul anului 2025, Autoritatea națională de supraveghere a formulat observații și propuneri pe marginea documentelor transmise de alte autorități/instituții:

- participare la proiectul cercetare al Agenției pentru Drepturi Fundamentale a Uniunii Europene (FRA) denumit „Directiva privind aplicarea legii (Law Enforcement Directive) – Implementarea practică și provocările cu care se confruntă autoritățile competente";
- propunerea de acord (Data Processing Agreement) între statul membru (în calitate de operator) și eu-LISA (în calitate de persoană împuternicită de operator);
- pachetul legislativ Omnibus IV – propunerea de regulament de modificare a Regulamentului (UE) 2016/679 prin extinderea derogării prevăzute la art. 30 alin. (5) din Regulamentul (UE);
- pachetul legislativ Omnibus VII – propunerea de regulament de modificare a Regulamentelor (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725, (UE) 2023/2854 și a Directivelor 2002/58/CE, (UE) 2022/2555 și (UE) 2022/2557 în ceea ce privește simplificarea cadrului legislativ digital și abrogarea Regulamentelor (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 și a Directivei (UE) 2019/1024 (Digital Omnibus)

Autoritatea națională de supraveghere a transmis o serie de observații în special cu privire la modificarea art. 4 pct. 1 din Regulamentul (UE) 2016/679, respectiv modificarea definiției conceptului de „date cu caracter personal", modificarea art. 5 lit. b (principiul „limitării legate de scop"), integrarea în cadrul Regulamentului (UE) 2016/679 a dispozițiilor prevăzute în Directiva 2002/58/CE (Directiva ePrivacy), precum și cu privire la introducerea art. 88a, 88b și 88c;

- planul de lucru 2026-2028 al Agenției pentru Drepturi Fundamentale a Uniunii Europene

Autoritatea națională de supraveghere a transmis comentarii pe marginea documentului transmis spre analiză, cu incidență asupra capitolului care vizează domeniul protecției datelor cu caracter personal;

- propunerea de Regulament de stabilire a unor norme procedurale suplimentare referitoare la asigurarea respectării Regulamentului (UE) 2016/679

Autoritatea națională de supraveghere a transmis, și în cursul anului 2025, o serie de observații și răspunsuri la întrebările adresate de Președinția Consiliului UE. Astfel,

Autoritatea națională de supraveghere a considerat că aplicarea Regulamentului (UE) 2016/679 și a acestui nou regulament ar trebui să primeze principiul unei cooperări loiale între autoritățile de supraveghere, astfel că orice nerespectare a unor termene procedurale ar trebui mai întâi să fie adusă la cunoștința celor în cauză de o manieră informală, înainte de a fi sesizat EDPB în mod oficial. Totodată, Autoritatea națională de supraveghere a apreciat ca fiind necesară reglementarea clară a atribuțiilor ce revin autorității de supraveghere principale (LSA) și autorității care a primit plângerea (CSA) în elaborarea deciziilor separate și distincte, destinate pe de o parte, operatorului și, pe de altă parte, petentului, în situația în care plângerea este admisă sau respinsă parțial, conform art. 60 alin. (9) din Regulamentul (UE) 2016/679. În plus, a fost subliniat faptul că sunt stabilite unele obligații suplimentare în sarcina autorităților de supraveghere, față de cele reglementate de Regulamentul (UE) 2016/679, acestea reprezentând sarcini administrative împovărătoare pentru autoritățile de supraveghere, care pot avea ca posibil efect tergiversarea soluționării unui caz într-un termen rezonabil. În ceea ce privește statisticile propuse prin regulament, Autoritatea națională de supraveghere a considerat că ar trebui definite mai bine criteriile în funcție de care se solicită aceste raportări, pentru o înțelegere și eventual implementare comună a acestora, subliniind faptul că realizarea unor astfel de statistici ar îngreuna activitatea Autorității naționale de supraveghere atât din punct de vedere tehnic și financiar, cât și din punct de vedere al resurselor umane. În luna noiembrie 2025, a fost publicat în Jurnalul Oficial la Uniunii Europene Regulamentul (UE) 2025/2518 al Parlamentului European și al Consiliului din 26 noiembrie 2025 de stabilire a unor norme procedurale suplimentare referitoare la asigurarea respectării Regulamentului (UE) 2016/679. Astfel, potrivit art. 37 din Regulamentul (UE) 2025/2518, acesta intră în vigoare în a douăzecea zi de la data publicării în Jurnalul Oficial al Uniunii Europene și se aplică de la 2 aprilie 2027.

- <u>propunerea de regulament a Parlamentului European și a Consiliului de instituire a Programului „AgoraUE" pentru perioada 2028–2034</u>

Având în vedere natura datelor cu caracter personal care pot face obiectului unei prelucrării în temeiul Regulamentului „Agora UE" pentru perioada 2028-2034, respectiv date cu caracter personal și categorii speciale de date cu caracter personal (date care dezvăluie originea rasială sau etnică, confesiunea religioasă sau convingerile filozofice, date privind viața sexuală sau orientarea sexuală), Autoritatea națională de supraveghere a

subliniat necesitatea respectării prevederilor Regulamentului (UE) 2016/679, în special în ceea ce privește principiile legate de prelucrarea datelor cu caracter personal prevăzute la art. 5, legalitatea prelucrării (art. 6), prelucrarea de categorii speciale de date cu caracter personal (art. 9), asigurarea respectării drepturilor persoanelor vizate prevăzute la art. 12-22, precum și instituirea de măsuri tehnice și organizatorice adecvate (art. 32).

➢ Acordul de prelucrare a datelor pentru schimbul electronic de informații privind securitatea socială în domeniul internațional EESSI (Electronic Exchange of Social Security Information)

Autoritatea națională de supraveghere a formulat o serie de observații pe marginea secțiunilor referitoare la persoanele vizate și categoriile de date, obligațiile și drepturile operatorului, obligațiile și drepturile persoanei împuternicite de operator, încălcările de securitatea a datelor.

**Misiunea de evaluare Schengen a României**

În anul 2025, potrivit Deciziei de punere în aplicare C(024) 5801 a Comisiei Europene, România a fost inclusă în programul de evaluare Schengen, misiunea de evaluare Schengen a României vizând inclusiv domeniul protecției datelor cu caracter personal.

În cadrul misiunii a fost evaluat stadiul de implementare a cerințelor în domeniul protecției datelor cu caracter personal în spațiul Schengen, având drept scop asigurarea faptului că statele membre aplică regulile Schengen în mod eficient și în conformitate cu principiile și normele fundamentale. În acest context, menționăm că Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal a fost evaluată de echipa de experți din perspectiva independenței instituționale și financiare, a atribuțiilor și competențelor, a asigurării și respectării drepturilor persoanelor vizate, precum și a realizării monitorizării și controlului legalității prelucrării datelor cu caracter personal în N.SIS (componenta națională a SIS) și în SNIV (Sistemul Național de Informații privind Vize).

**În urma misiunii de evaluare Schengen în domeniul protecției datelor cu caracter personal, echipa de experți a emis o serie de recomandări către România, printre care evidențiem recomandarea ca Autoritatea națională de supraveghere să dispună de resurse umane, financiare și tehnice suficiente, pentru exercitarea în mod eficient a responsabilităților și sarcinilor legate de Sistemul de Informații Schengen (SIS) și Sistemul de Informații privind Vizele (VIS).**

## CAPITOLUL V

## MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfășurării activității, potrivit Legii nr. 9/2025 a bugetului de stat pe anul 2025, Autorității naționale de supraveghere i s-a alocat un buget inițial pe anul 2025 în sumă de 6.001.000 lei.

Ulterior, în urma rectificărilor bugetare realizate potrivit prevederilor Ordonanțelor de Urgență ale Guvernului nr. 50/2025 și nr. 64/2025, bugetul autorității a fost majorat la titlul 10 Bunuri și servicii cu 100.000 lei.

După realizarea anulărilor de credite bugetare din luna decembrie, potrivit prevederilor Legii nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare, bugetul final pe anul 2025 al Autorității a fost în sumă de 6.091.000 lei și a avut următoarea structură:

- Cap. 51.01 Autorităţi executive și legislative – 6.091.000 lei
- Cheltuieli curente – 6.091.000 lei
- Titlul I Cheltuieli de personal – 4.991.000 lei
- Titlul II Bunuri şi servicii – 1.100.000 lei
- Cheltuieli de capital – 0 lei
- Titlul XIII Active nefinanciare – 0 lei

Creditele definitive aprobate au asigurat funcționarea instituției în anul 2025, în condiții de restricții bugetare, potrivit reglementărilor în vigoare.

| Anul | 2021 | 2022 | 2023 | 2024 | 2025 |
|---|---|---|---|---|---|
| Buget final (mii lei) | 4.601 | 5.580 | 5.595 | 5.714 | 6.091 |
| % fata de anul anterior | 93,84% | 121,27% | 100,26% | 102,13% | 106,60% |

Bugetul final al autorității pe anul 2025 a înregistrat o ușoară creștere raportat la bugetul anului 2024, aceasta fiind necesară atât pentru acoperirea cheltuielilor cu drepturile de personal (așa cum au fost acestea stabilite de legiuitor în urma creșterilor

succesive prevăzute de actele normative aprobate în anul 2024), cât și pentru asigurarea unui nivel minim necesar al cheltuielilor înregistrate la Titlul Bunuri și servicii.

Evidențiem că, urmare a restricțiilor bugetare stricte, Autoritatea națională de supraveghere a înregistrat în anul 2026, pentru prima dată de la înființare, plăți restante. Cu toate acestea, eforturile depuse de reprezentanții Autorității naționale de supraveghere au făcut ca aceste plăți restante să nu se transforme în arierate.

Un factor semnificativ în dezechilibrarea bugetului Autorității naționale de supraveghere l-au reprezentat cheltuielile aferente contractului de locațiune cu RAPPS și, în mod special, creșterile semnificative ale sumelor reprezentând contravaloarea utilităților și prestări servicii aferente contractului de închiriere.

Cu privire la faza de programare bugetară, precizăm faptul că Autoritatea națională de supraveghere a avut în vedere obiectivele stabilite pentru anul 2025, iar limitările bugetare impuse de către Ministerul Finanțelor, pe baza cărora s-a fundamentat necesarul inițial de fonduri, au determinat aprobarea unui buget inițial pentru instituția noastră în sumă de 5.990.000 lei.

Evoluția macroeconomică nefavorabilă din anul 2025 a generat necesitatea solicitării de fonduri suplimentare. Autoritatea națională de supraveghere a fundamentat și a transmis necesarul de fonduri suplimentare către instituțiile abilitate, astfel încât, cu ocazia rectificărilor bugetare, s-a realizat majorarea bugetului Autorității naționale de supraveghere cu 100 mii lei la titlul 10 Bunuri și servicii.

În urma modificărilor de alocări bugetare realizate prin actele normative de rectificare a bugetului de stat pe anul 2025 și în urma anulărilor de credite realizate în luna decembrie 2025, potrivit reglementărilor Legii nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare, situația bugetului Autorității naționale de supraveghere și execuția bugetară din anul 2025 se prezintă potrivit următorului tabel sintetic:

| Denumire indicator | Cod | Buget inițial 2025 - mii lei - | Buget final (actualizat la 31.12.2025) - mii lei - | Execuție bugetară la 31.12.2025 - mii lei - | Execuţie bugetară la 31.12.2025 (%) |
|---|---|---|---|---|---|
| Total cheltuieli | 51.01 | 6.001 | 6.091 | 6.078,08 | 99,79 |
| Titlul I Cheltuieli de personal | 10 | 5.001 | 4.991 | 4.985,70 | 99,89 |
| Titlul II Bunuri şi servicii | 20 | 1.000 | 1.100 | 1.091,37 | 99,22 |
| Cheltuieli de capital Titlul XIII Active nefinanciare | 71 | 0 | 0 | 0 | 0 |

Este de precizat faptul că, în anul 2025, au fost recuperate sume din cheltuieli realizate în anii precedenți în valoare de 175.766,46 lei reprezentând, în principal, sume recuperate de la CASMB aferente cererilor de recuperare FNUASS depuse de autoritate în anii anteriori (2023-2024), acestea fiind transferate la bugetul de stat, potrivit reglementărilor legale în vigoare.

Menționăm faptul că în anul 2025 Autoritatea națională de supraveghere s-a confruntat, în continuare, cu o lipsă acută de personal, instituția desfășurându-și activitatea la finalul anului 2025 cu un număr de doar 33 de salariați contractuali și 2 demnitari.

Creditele aprobate prin buget la Titlul 10 " Cheltuieli de personal" au asigurat plata integrală a drepturilor de personal în anul 2025 pentru un număr mediu de 36 de persoane (inclusiv demnitarii).

Numărul mediu de posturi ocupate (36) în anul 2025 s-a menținut la același nivel cu anul 2024 și reprezintă un procent de doar 41% din numărul total de posturi prevăzut în legea de organizare (87 de posturi).

Angajarea cheltuielilor de personal s-a efectuat în baza prevederilor legale, respectiv:

- Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată, cu modificările și completările ulterioare;
- Legea-cadru nr. 153 din 28 iunie 2017 privind salarizarea personalului plătit din fonduri publice, cu modificările și completările ulterioare;
- Legea nr. 9/2025 a bugetului de stat pe anul 2025, Ordonanțele de Urgență ale Guvernului nr. 50/2025 și nr. 64/2025 cu privire la rectificarea bugetului de stat pe anul 2025;
- Ordonanța de Urgență a Guvernului nr. 156/2024 privind unele măsuri fiscal-bugetare în domeniul cheltuielilor publice pentru fundamentarea bugetului general consolidat pe anul 2025, pentru modificarea și completarea unor acte normative, precum și pentru prorogarea unor termene, cu modificările și completările ulterioare și Ordonanța de Urgență nr. 36/2025 pentru stabilirea unor măsuri privind personalul plătit din fonduri publice.

La titlul 20 "Bunuri și servicii" sumele alocate prin buget au asigurat un minim necesar pentru desfășurarea activității Autorității naționale de supraveghere, iar pe parcursul exercițiului bugetar, așa cum s-a precizat anterior, a fost constatată necesitatea alocării de fonduri suplimentare, astfel încât Autoritatea națională de supraveghere a fundamentat și transmis o solicitare către instituțiile abilitate, fiindu-i alocată suplimentar suma de 100 mii lei la titlul 10 Bunuri și servicii, cu prilejul rectificării bugetare aprobate prin Ordonanța de Urgență ale Guvernului nr. 50/2025.

Angajarea cheltuielilor cu bunuri și servicii a avut la bază actele și documentele justificative, respectiv contracte de prestări servicii, achiziții de bunuri, note de fundamentare aprobate de ordonatorul principal de credite și s-a făcut în baza Legii nr. 98/2016 privind achizițiile publice și a celorlalte reglementări specifice, raportat și la restricțiile aplicabile în anul 2025 în ceea ce privește achizițiile.

Pe parcursul anului 2025 o influență semnificativă asupra cheltuielilor cu bunuri și servicii au avut creșterile de prețuri, în mod special cele ale utilităților și ale prestărilor de servicii aferente contractului de locațiune dintre Autoritatea națională de supraveghere și RA APPS - SAIFI.

Subliniem faptul că, în anul 2025, au fost permanent ajustate necesitățile instituției privind cheltuielile cu bunuri și servicii (inclusiv cele pentru servicii și produse IT), avându-se în vedere restricțiile bugetare impuse, încadrarea în creditele bugetare și creditele bugetare alocate potrivit bugetului aprobat al Autorității naționale de supraveghere și în limitele lunare de credite de angajament și credite bugetare aprobate potrivit actelor normative în vigoare.

În ceea ce privește evidența contabilă, menționăm că aceasta a fost ținută la zi, urmărindu-se atât legalitatea și oportunitatea cheltuielilor bugetare, cât și utilizarea sumelor alocate cu maximum de eficiență posibilă, într-o perioadă ce a continuat să fie influențată semnificativ de restricții bugetare.