AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

R A P O R T A N U A L

2024

Raportul de activitate este transmis Senatului României, Camerei Deputaților, Guvernului României, Comisiei Europene și Comitetului European pentru Protecția Datelor, în temeiul 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,

Îmi revine deosebita onoare de a vă prezenta Raportul de activitate al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, pentru anul 2024, prin care s-au evidențiat principalele direcții de acțiune în activitatea de monitorizare și control din domeniul protecției datelor personale.

Anul 2024 a reprezentat o perioadă de consolidare în asigurarea aplicării eficiente a Regulamentului (UE) 2016/679 privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date, împreună cu celelalte reglementări naționale specifice din acest domeniu.

În acest context de dezvoltare tehnologică accentuată, respectarea pe scară largă a regulilor de folosire a datelor personale a reprezentat un obiectiv esențial reflectat în toate componentele activității instituției noastre.

În ceea ce privește activitatea de monitorizare și control, reliefăm că, în anul 2024, au continuat acțiunile de control în sectorul public și privat, care s-au concretizat în măsuri corective dispuse operatorilor, destinate îmbunătățirii activității acestora pe termen mediu și lung.

Creșterea nivelului de conștientizare a publicului larg și preocuparea constantă a operatorilor din mediul public și privat de a asigura respectarea condițiilor de prelucrare a datelor personale, au constituit și în acest an elemente de evidențiat prin raportare la activitatea Autorității naționale de supraveghere.

Cooperarea cu celelalte autorități naționale de protecția datelor din Uniunea Europeană a continuat în aceiași parametri, inclusiv prin reprezentarea la nivelul Comitetului European pentru Protecția Datelor, destinată analizării situațiilor cu impact transfrontalier și a transferurilor.

În considerarea activității desfășurate în anul 2024, concluzionăm că, raportat la constrângerile bugetare existente și la resurse umane limitate, au fost îndeplinite obiectivele instituției noastre de asigurare adecvată a monitorizării și controlului în domeniul protecției datelor cu caracter personal.

Pe termen mediu, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal își propune intensificarea activității de monitorizare și control a operatorilor, soluționarea corespunzătoare a plângerilor primite, continuarea activităților de informare publică a persoanelor fizice, operatorilor și mass-mediei, corelat cu resursele disponibile, în vederea asigurării unei aplicări adecvate a Regulamentului (UE) 2016/679 și a celorlalte acte normative incidente.

În final, aș dori să vă mulțumesc pentru sprijinul constant acordat instituției noastre și să-mi exprim încrederea că vom beneficia și pe viitor de susținerea dumneavoastră, în îndeplinirea rolului nostru de asigurare a unei efective exercitări a dreptului la protecția datelor cu caracter personal în România.

Ancuța Gianina OPRE,

PREȘEDINTE

CUPRINS

CAPITOLUL I

PREZENTARE GENERALĂ

Raportul de activitate pe anul 2024 al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea naţională de supraveghere) este structurat pe șase capitole, astfel:

Capitolul I conține o panoramare sintetică a principalelor activități în care s-a concretizat exercitarea competențelor legale ale Autorității naționale de supraveghere, astfel încât să se asigure o reflectare adecvată a direcțiilor de acțiune.

În considerarea dezideratului de a se realiza respectarea regulilor specifice domeniului protecției datelor cu caracter personal, activitatea instituției s-a concentrat pe liniile de acțiune necesare pentru monitorizarea și controlul aplicării principiilor de prelucrare, de îmbunătățire a gradului de informare a publicului larg și de asigurare a cooperării cu celelalte autorități naționale și europene.

În cadrul **Capitolului al II-lea** sunt cuprinse principalele aspecte ce reflectă activitatea de avizare a proiectelor de acte normative, de autorizare şi de consiliere a operatorilor, de informare publică, în concordanță cu competențele stabilite de Regulamentul (UE) 2016/679 și de celelalte acte normative în domeniu. Această activitate a implicat, în principal, formularea de avize asupra unui număr semnificativ de proiecte de acte normative şi în transmiterea de puncte de vedere referitoare la aplicarea corespunzătoare a prevederilor din domeniul protecției datelor. Sub acest aspect, reliefăm că persoanele fizice şi operatorii de date din sectorul privat și din cel public au continuat să își exprime interesul pentru aplicarea adecvată a reglementărilor din materia protecției datelor și au solicitat numeroase punct de vedere cu privire la aplicabilitatea Regulamentului (UE) 2016/679, în diferite domenii și situații complexe.

De asemenea, în această secțiune sunt disponibile informații relevante privind cele mai importante litigii finalizate pe parcursul anului 2024, 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 2024, raportat la investigaţiile efectuate, însoțite de principalele date statistice.

Astfel, în ceea ce privește investigaţiile 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, în principal, pierderea confidențialității și accesul neautorizat a datelor cu caracter personal inclusiv în mediul online, confidențialitatea datelor cu caracter personal prin nerespectarea principiului privacy by design/privacy by default, prelucrarea datelor cu caracter personal ale clienților din sistemul bancar, accesul neautorizat la sistemele de supraveghere video, divulgarea neautorizată a datelor cu caracter personal.

Referitor la componenta de soluționare a plângerilor și a sesizărilor, menționăm că, în anul 2024, 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 o serie de exemple cu cele mai relevante cazuri din controalele care au avut loc.

În cursul anului 2024, 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 aspecte relevante din activitatea de relaţii externe a Autorităţii naţionale de supraveghere, prin prezentarea diferitelor documente adoptate la nivelul Uniunii Europene, cu aplicabilitate în domeniul protecției datelor personale, alături de elemente semnificative referitoare la transferul acestora.

În același timp, este prezentată și cooperarea cu alte autorități de supraveghere din Uniunea Europeană în vederea asigurării asistenței reciproce, precum și informații utile privind contribuția instituției noastre în relația cu organismele europene.

Capitolul al V-lea conține cele mai importante informații privind managementul economic al instituției, respectiv creditele bugetare puse la dispoziția Autorității naţionale de supraveghere, precum şi cheltuielile aferente, de natură a contura o imagine de ansamblu cu privire la resursele bugetare disponibile în anul 2024.

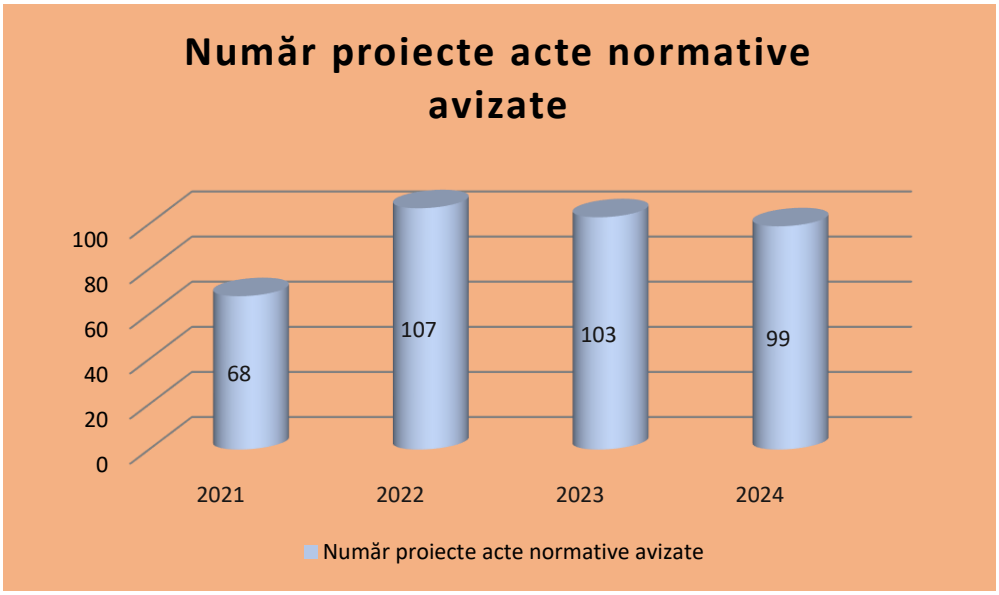
Față de aspectele prezentate în cadrul fiecărui capitol, raportat la obiectivele Autorității naționale de supraveghere, rezultă că s-au făcut eforturi deosebite ale personalului instituției noastre pentru ca activitatea în anul 2024 să se desfășoare în parametri corespunzători, în condițiile în care resursele umane și financiare de care am dispus au fost deficitare.

Pe viitor, instituția noastră își propune continuarea activității de monitorizare și control al operatorilor, soluționarea corespunzătoare a plângerilor primite, continuarea activităților de informare publică, raportat și la resursele disponibile, în vederea asigurării unei aplicări adecvate a Regulamentului (UE) 2016/679 și a celorlalte acte normative aplicabile în domeniul protecției datelor cu caracter personal.

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

Secțiunea 1
Avizarea actelor normative

În anul 2024, 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 **99 de proiecte de acte normative** transmise de instituţii publice, care implicau aspecte diferite privind prelucrarea datelor cu caracter personal.



Proiectele de acte normative au fost transmise de către anumite ministere, precum Ministerul Afacerilor Interne, Ministerul Justiției, Ministerul Sănătății, Ministerul Muncii și Solidarității Sociale, Ministerul Educației, Ministerul Dezvoltării, Lucrărilor Publice și Administrației, Ministerul Finanțelor, 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 Muncii și Solidarității Sociale a solicitat Autorității naționale de supraveghere un punct de vedere asupra proiectului de Hotărâre a Guvernului pentru aprobarea Normelor de aplicare a prevederilor Legii nr. 360/2023 privind sistemul public de pensii**

Față de conținutul proiectului de act normativ, Autoritatea națională de supraveghere a propus includerea unui articol în sensul că prelucrarea datelor cu caracter personal se va efectua cu respectarea 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.

De asemenea, Autoritatea Națională de Supraveghere a propus introducerea în cadrul fiecărei anexe (cerere) din cadrul proiectului de act normativ a informațiilor prevăzute de art. 12 și art. 13 din Regulamentul (UE) 679/2016, având în vedere necesitatea respectării dreptului la informare al persoanei vizate.

- **Secretariatul General al Guvernului a transmis propunerea legislativă pentru modificarea și completarea unor acte normative în domeniul siguranței publice, în vederea formulării unui punct de vedere.**

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

La art. I din propunerea legislativă referitoare la modificarea și completarea Ordonanţei de Urgenţă nr. 104/2001 privind organizarea şi funcţionarea Poliției de Frontieră Române, au fost formulate, în principal, următoarele propuneri:

- La pct. 2 s-a apreciat ca fiind necesară precizarea acelor ”alte mijloace tehnice din dotare” la care se face referire în text;

- La pct. 3 s-a recomandat reanalizarea prevederii în considerarea principiului potrivit căruia datele trebuie să fie adecvate, relevante şi limitate la ceea ce este necesar (neexcesive) prin raportare la scopurile în care sunt prelucrate, stabilit de Regulamentul (UE) 2016/679, corelat cu dispozițiile din Legea nr. 363/2018 (art. 5 alin. (1) lit. c) din cele două acte normative menționate);

- S-a considerat că este necesară reanalizarea dispozițiilor pct. 6, respectiv a lit. b) din alin. (1) al art. 3^2 din propunerea legislative, referitoare la utilizarea de către Poliția de Frontieră de mijloace foto-audio-video sau alte mijloace tehnice din dotare, ocazional.

În consecință, în contextul celor de mai sus, a rezultat că este necesar ca prelucrările de date prin mijloacele foto-audio-video și alte mijloace tehnice din dotarea Poliției de Frontieră să fie clar identificate, textul să conțină prevederile necesare care să abiliteze entitatea menționată să utilizeze astfel de mijloace în activitatea derulată de angajații săi, raportat și la respectarea principiilor de prelucrare a datelor prevăzute de Regulamentul (UE) 2016/679, respectiv de Legea nr. 363/2018.

- S-a subliniat că este necesară reanalizarea dispozițiilor pct. 6, respectiv a alin. (2) al art. 3^2 din propunerea legislativă referitoare la autorizarea Poliției de Frontieră să acceseze în mod direct sistemele de supraveghere a spațiilor publice instalate în scopul prevenirii criminalității, pazei bunurilor și protecției persoanelor sau supravegherii traficului rutier și care aparțin organelor administrației publice centrale sau locale.

Față de aceste prevederi, s-a menționat faptul că art. 1 alin. (2) din Legea nr. 363/2018 prevede că prelucrarea datelor cu caracter personal pentru realizarea activităţilor de menţinere şi asigurare a ordinii şi siguranţei publice se realizează numai dacă acestea sunt prevăzute de lege şi sunt necesare pentru prevenirea unui pericol cel puţin asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea infracţiunilor.

De asemenea, art. 6 din aceeași lege prevede că prelucrările de date cu caracter personal în scopul realizării activităţilor prevăzute la art. 1 din lege, inclusiv cele bazate pe

utilizarea noilor tehnologii sau care sunt de natură să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice se instituie prin acte normative.

Art. 5 din Legea nr. 363/2018 stabilește principiile de prelucrare a datelor, printre care se numără cele privind prelucrarea de date adecvate, relevante şi neexcesive prin raportare la scopurile în care sunt prelucrate, prelucrarea de date exacte și păstrarea datelor într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele respective.

De asemenea, art. 5 din Legea nr. 363/2018 statuează că datele cu caracter personal pot fi prelucrate pentru realizarea activităţilor prevăzute la art. 1 din lege, de către acelaşi operator sau de către alt operator într-un alt scop decât cel avut în vedere la momentul colectării datelor cu caracter personal, numai dacă sunt îndeplinite cumulativ următoarele condiţii:

- operatorul este abilitat să prelucreze astfel de date cu caracter personal în scopul respectiv, în conformitate cu cadrul normativ aplicabil;

- prelucrarea este necesară şi proporţională în raport cu scopul respectiv, în conformitate cu cadrul normativ aplicabil.

În acest context, s-a subliniat că sunt incidente și dispozițiile art. 35 din Regulamentul (UE) 2016/679 coroborate cu art. 32 și art. 33 din Legea nr. 363/2018, cu privire la evaluarea impactului asupra protecției datelor.

În același timp, întrucât prelucrarea datelor implică o prelucrare ulterioară a datelor personale deținute de autorități publice locale sau centrale, raportat și la dispozițiile art. 8 din Legea nr. 363/2018, s-a subliniat faptul că art. 6 alin. (4) din Regulamentul (UE) 2016/679 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.

- Cât privește pct. 6, cu referire la alin. (3) al art. 3^2 s-a subliniat că este necesar ca actul normativ a cărui modificare/completare se intenționează prin propunerea de act normativ, să cuprindă reglementări exprese referitoare la garanțiile necesare pentru protejarea drepturilor persoanelor vizate (de ex. modalitatea de exercitarea drepturilor prevăzute de Regulamentul (UE) 2016/679, precum și de Legea nr. 363/2018).

În ceea ce privește modificările și completările preconizate a fi aduse atât Legii nr. 550/2004 privind organizarea şi funcţionarea Jandarmeriei Române (Art. II din propunerea

legislativă), cât și Ordonanței de Urgență nr. 55/2007 privind înființarea Oficiului Român pentru Imigrări prin reorganizarea Autorităţii pentru Străini și a Oficiului Național pentru Refugiați, precum și modificarea și completarea unor acte normative (Art. III din propunerea de act normativ), respectiv Ordonanței de Urgență nr. 30/2007 (Art. IV din propunerea legislativă) s-a subliniat că acestea sunt similare sau identice celor ce se intenționează a fi aduse Ordonanţei de Urgenţă nr. 104/2001.

Ca atare, Autoritatea națională de supraveghere a menținut observațiile anterioare și în cazul modificărilor și completărilor ce ar urma să fie aduse actelor normative supuse modificării prin prezentul proiect.

- **Ministerul Justiției a solicitat formularea unui punct de vedere asupra proiectului de Lege pentru modificarea și completarea Legii cetățeniei române nr. 21/1991, precum şi pentru modificarea şi completarea altor acte normative**.

Faţă de conţinutul proiectului de act normativ afișat pe site-ul Ministerului Justiției, raportat la dispozițiile Regulamentului (UE) 2016/679, s-a recomandat reanalizarea prevederilor Art. I pct. 20 din proiect referitoare la completarea art. 20 cu alin. (5) lit. c) cu privire la faptul că personalul din cadrul Autorității Naționale pentru Cetățenie sau, după caz, al misiunii diplomatice sau oficiului consular ”obține acordul scris al persoanei care urmează să depună jurământul de credință cu privire la caracterul complet și exact al datelor cu caracter personal, altele decât cele biometrice, necesare personalizării cardului de cetățenie română, acord ce va fi exprimat atât pentru sine, cât și pentru copiii minori pentru care persoana respectivă a solicitat acordarea sau redobândirea cetățeniei române.”

Autoritatea naţională de supraveghere a formulat o observație cu titlu general, raportat la întreg textul proiectului de act normativ, întrucât (re)dobândirea cetățeniei române presupune o multitudine de operațiuni de prelucrări de date cu caracter personal (inclusiv date cu caracter special – date biometrice), precum și crearea unui ”dosar electronic al solicitantului” (Art. I pct. 35 din proiect), respectiv crearea unui sistem informatic de evidență a cardurilor de cetățenie română și a unei platforme informatice care conține date cu caracter personal.

Astfel, s-a recomandat clarificarea utilizării noțiunii de sistem informatic de evidență a cardurilor de cetățenie română, respectiv a unei platforme informatice, precum și introducerea în actele normative completate și modificate prin proiectul supus analizei, respectiv în Legea nr. 21/1991 și în O.U.G. nr. 5/2010, a câte unui articol distinct care să conțină prevederi în sensul aplicării tuturor dispozițiilor Regulamentului (UE) nr. 679/2016 și a celorlalte acte normative aplicabile domeniului protecției datelor, în legătură cu prelucrările de date efectuate de către toate entitățile implicate în activitățile reglementate de actul normativ supus avizării.

Autoritatea naţională de supraveghere a avizat forma finală a proiectului având în vedere faptul că au fost preluate observațiile și propunerile instituției noastre.

- **Ministerul Mediului, Apelor și Pădurilor a transmis Autorității naționale de supraveghere proiectul de Lege privind Codul silvic**

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:

Referitor la dispozițiile art. 97 din proiect referitor la utilizarea instrumentelor și tehnologiilor moderne de supraveghere, prin care se introduc reglementări referitoare la prelucrarea de date cu caracter personal prin mijloace de supraveghere audio-video, s-a evidențiat că trebuie să conțină dispoziții clare referitoare la:

- condițiile generale care reglementează legalitatea prelucrării prin utilizarea de mijloace de supraveghere video de către operatorii de date menționați în art. 97, respectiv fiecare administrator de fond forestier și autoritatea publică centrală pentru silvicultură (instituție care ar asigura conectarea sistemelor de monitorizare instalate de structurile de administrare ale fondului forestier la sistemul informațional integrat pentru păduri) care ar avea obligații să utilizeze în activitatea lor de asigurare a integrităţii fondului forestier național, de prevenire şi combatere a activităţilor ilegale şi de asigurare a trasabilității lemnului recoltat din pădure, de administrare a mijloacelor de probă;

- tipurile de date care fac obiectul prelucrării, întrucât din conținutul proiectului nu reiese cu claritate dacă sunt prelucrate doar imagini preluate prin sisteme de supraveghere

video sau și alte date care pot fi prelucrate prin utilizarea acelorași sisteme care pot avea caracteristici tehnice avansate);

- persoanele vizate, întrucît acestea sunt atât persoanele fizice care pot fi înregistrate video, cât și angajații administratorilor de fond forestier sau persoanele cu atribuții de pază, menționate la art. 92 alin. (5) și (10) din proiectul de cod;

- perioada maximă de stocare a datelor;

De asemenea, s-a menționat considerentul (41) din Regulamentul (UE) 2016/679 care stabilește faptul că o măsura legislativă trebuie să fie clară şi precisă, iar aplicarea acesteia ar trebui să fie previzibilă pentru persoanele vizate de aceasta, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene ("Curtea de Justiție") și a Curții Europene a Drepturilor Omului.

Totodată, art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679 stabilește principiul potrivit căruia datele cu caracter personal trebuie să fie adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor"), iar din prezentul proiect de act normativ nu rezultă că este respectată această cerință.

Autoritatea naţională de supraveghere a subliniat că prelucrarea datelor prin mijloace de supraveghere video nu constă doar în prelucrarea imaginii angajaților entităților cu atribuții de pază a fondului forestier din România, ci și în prelucrarea datelor tuturor persoanelor fizice, care au acces la fondul forestier (de ex. turiști), ceea ce reprezintă o prelucrare pe scară largă a unor zone accesibile publicului, prelucrare aflată sub incidența art. 35 din Regulamentul (UE) 2016/679.

În acest sens, s-a subliniat că art. 35 alin. (1) din Regulamentul (UE) 2016/679 prevede faptul că, 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, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal.

În ceea ce privește drepturile persoanelor vizate, s-a atras atenția asupra faptului că este necesar să se respecte prevederile Regulamentului (UE) 2016/679, precum și cele ale Legii nr. 363/2018 (raportat la activitățile de prevenire și combatere a activităților ilegale legate de fondul forestier).

De asemenea, în contextul în care prevederile proiectului de cod conțin reglementări care presupun efectuarea de prelucrări de date cu caracter personal, s-a propus introducerea unui nou articol în textul proiectului referitor la aplicarea Regulamentului (UE) 2016/679 și a celorlalte acte normative aplicabile domeniului protecției datelor, în legătură cu prelucrările de date efectuate de către toate entitățile implicate în activitățile reglementate de actul normativ supus avizării.

- **Secretariatul General al Guvernului a transmis proiectul de Lege pentru completarea Ordonanței de urgență a Guvernului nr. 57/2019 privind Codul administrativ**

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

Cu privire la prevederile art. 47^{11} din proiect referitor la administrarea și funcționarea Registrului Unic al Transparenței Intereselor (RUTI) - platformă publică online, s-a subliniat faptul că aceasta presupune, printre altele, efectuarea de prelucrări de date cu caracter personal (conform alin. 4), prelucrări care intră sub incidența Regulamentului (UE) 2016/679, respectiv a Legii nr. 190/2018.

Autoritatea naţională de supraveghere a considerat că este necesară completarea proiectului de act normativ cu o prevedere potrivit căreia gestionarea Registrului se va realiza cu respectarea Regulamentului (UE) 2016/679, a Legii 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 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), cu modificările ulterioare, precum și a legislaţiei naţionale privind domeniul protecţiei datelor cu caracter personal.

De asemenea, s-a apreciat ca fiind necesară adăugarea garanțiilor prevăzute de Regulamentul (UE) 2016/679 în ceea ce privește prelucrarea datelor cu caracter personal, precum și particularizarea acestora la situațiile specifice din proiect, raportat și la prelucrările online implicate.

S-a menționat faptul că precizarea datelor, respectiv a categoriilor de date cu caracter personal care sunt prelucrate prin intermediul RUTI, este necesară în vederea respectării

principiilor legate de prelucrarea datelor, stabilite de art. 5 din Regulamentul (UE) 2016/679, în vederea respectării prevederilor Legii nr. 24/2000, cu modificările și completările ulterioare, raportat și la jurisprudența constantă a Curții Constituționale a României.

Totodată, în lumina celor de mai sus, deși prin RUTI se intenționează reglementarea unui caracter transparent al activității tuturor persoanelor prevăzute la art. 47^2 din proiect și al unor persoane terţe ce ar putea influența luarea unei decizii, s-a subliniat faptul că este necesară asigurarea unui just echilibru cu interesul reprezentat de protecţia datelor cu caracter personal și prevalența necesității asigurării confidenţialităţii acestor date.

Ca atare, s-a apreciat că se impune o analiză în sensul celor anterior precizate, care să se regăsească în Nota de fundamentarea a actului normativ.

În ceea ce privește responsabilitatea operatorului, au fost menționate și prevederile art. 24 din Regulamentul (UE) 2016/679 și, în același timp s-a subliniat faptul că este necesar să fie incluse în actul normativ prevederi referitoare la măsurile tehnice și organizatorice adecvate și eficiente, aplicabile în activitatea de gestionare a RUTI.

De asemenea, s-a precizat că, la configurarea RUTI, se vor avea în vedere garanțiile necesare pentru punerea în aplicare a principiilor menite să protejeze drepturile persoanelor vizate ale căror date vor fi înscrise în RUTI, potrivit principiilor statuate de art. 25 din Regulamentul (UE) 679/2016 privitoare la principiul protejării datelor cu caracter personal începând cu momentul conceperii lor și în mod implicit (privacy by design and by default), respectiv ale prevederilor art. 32 din Regulamentul (UE) 2016/679 referitoare la securitatea prelucrărilor.

În contextul celor de mai sus, a rezultat că este necesară reanalizarea și completarea proiectului de act normativ transmis, raportat la observațiile și propunerile formulate.

- **Secretariatul General al Guvernului a transmis Autorității naționale de supraveghere propunerea legislativă privind obligativitatea folosirii camerelor de corp în timpul controalelor şi/sau inspecţiilor realizate de către instituţiile publice de control din România**

Raportat la textul propunerii legislative, prin care se intenționează utilizarea de camere video portabile (mijloace de supraveghere audio-video de tip body-cam) de către toate instituțiile publice din România care au atribuții de control în legătură cu derularea activităților

de control ale acestora, s-a precizat că aceasta nu întrunește condițiile prevăzute de art. 6 alin. (3) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulația a acestor date.

Astfel, introducerea unei reglementări referitoare la prelucrarea de date cu caracter personal prin mijloace de supraveghere audio-video precum cele menționate, cu un impact major asupra vieții private, trebuie să conțină dispoziții clare referitoare la:

- condițiile generale care reglementează legalitatea prelucrării de către operatorii de date, respectiv de către fiecare instituție cu atribuții de control care ar fi obligată, potrivit propunerii în discuție, să utilizeze în activitatea derulată astfel de mijloace portabile de supraveghere audio video;

- tipurile de date care fac obiectul prelucrării;

- persoanele vizate; față de acest aspect subliniem că persoane vizate sunt atât persoanele fizice care pot fi înregistrate audio-video cât și angajații instituțiilor de control la care face referire propunerea legislativă.

- entitățile cărora le pot fi divulgate datele și scopul pentru care respectivele date cu caracter personal pot fi divulgate;

- limitările legate de scop, raportat la principiul de prelucrarea a datelor personale stabilit prin dispozițiile art. 5 alin. (1) lit. b) din Regulamentul (UE) 2016/679;

- perioadele de stocare; potrivit art. 5 alin. (1) lit. e) din Regulamentul (UE) 2016/679, datele trebuie *"păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele".*

- operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile cum sunt cele pentru alte situații concrete de prelucrare, astfel cum sunt prevăzute în capitolul IX din Regulamentul (UE) 2016/679.

De asemenea, considerentul (41) din Regulamentul General privind Protecția Datelor stabilește faptul că o măsura legislativă trebuie să fie clară şi precisă, iar aplicarea acesteia ar trebui să fie previzibilă pentru persoanele vizate de aceasta, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene ("Curtea de Justiție") și a Curții Europene a Drepturilor Omului.

Autoritatea națională de supraveghere a subliniat că prelucrarea datelor prin mijloace audio-video nu constă doar în prelucrarea imaginii/vocii angajaților instituțiilor cu atribuții de control din România, ci și în prelucrarea datelor tuturor persoanelor fizice, cetățeni (inclusiv minori, persoane cu dizabilități, etc.), cu care acești angajați intră în contact în timpul exercitării atribuțiilor de serviciu, ceea ce reprezintă o prelucrare pe scară largă aflată sub incidența art. 35 din Regulamentul (UE) 679/2016.

În acest sens, s-a precizat că art. 35 alin. (1) din Regulamentul (UE) 679/2016 prevede faptul că, 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, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal. O evaluare unică poate aborda un set de operaţiuni de prelucrare similare care prezintă riscuri ridicate similare.

În același timp, raportat la reglementările din propunerea legislativă, s-a subliniat că, prin raportare la dispozițiile alin. (10) al art. 35 din Regulamentul (UE) 2016/679, 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 garanţii, fapt de natură a afecta viața privată a tuturor persoanelor fizice, nu doar a celor controlate de toate instituţiile din România care au atribuții de control și care ar fi obligate prin această propunere legislativă, să utilizeze astfel de mijloace intruzive de supraveghere audio-video.

În același timp, în ceea ce privește respectarea drepturilor persoanelor vizate, s-a atras atenția că este necesar să se respecte prevederile Regulamentului (UE) 2016/679.

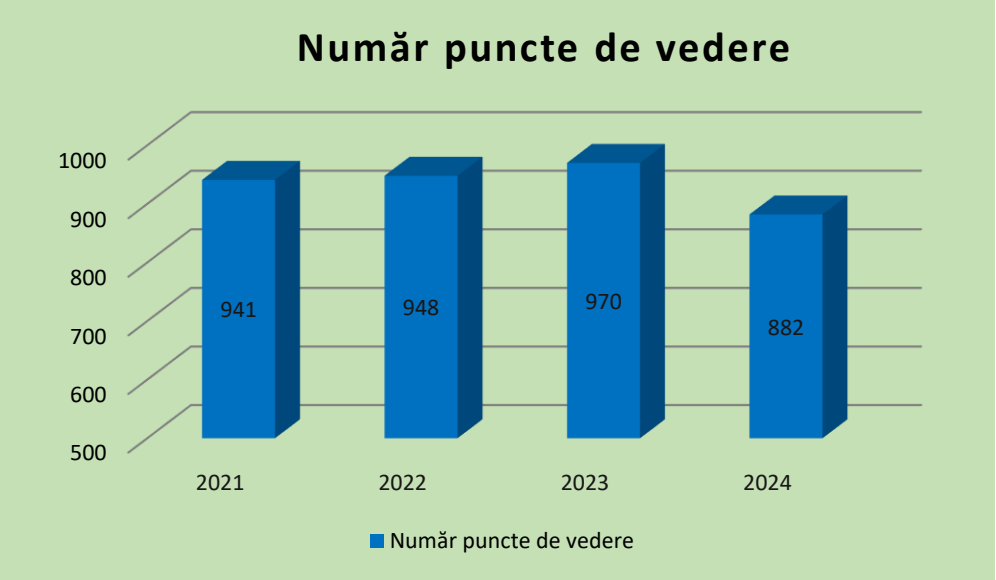
Autoritatea națională de supraveghere nu a susținut această propunere legislativă.

Secțiunea a 2-a:

Puncte de vedere

În anul 2024 a fost adresat Autorității naționale de supraveghere un număr de **882 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.

Și în acest an se poate observa că numărul de solicitări s-a menținut la un nivel semnificativ, ceea ce ilustrează un interes constant atât al operatorilor și împuterniciților în asigurarea respectării regulilor de prelucrare a datelor personale instituite de Regulamentul (UE) 2016/679 și de legislația națională specifică, cât și 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:

♦ Anonimizarea datelor privind domiciliul dintr-o declarație de avere

O persoană fizică a solicitat un punct de vedere referitor la prevederile legale aplicabile în contextul în care aceasta dorea anonimizarea datelor privind domiciliul dintr-o declarație de avere.

Având în vedere conținutul adresei, Autoritatea națională de supraveghere a formulat următoarele precizări:

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

Astfel, s-a menționat că art. 6 din Regulamentul (UE) 2016/679 stabilește că prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre condițiile prevăzute de aceste dispoziții, printre care se numără cea în care prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului (art. 6 alin. (1) lit. c) din Regulamentul (UE) 2016/679).

De asemenea, s-a precizat faptul că art. 5 din Regulamentul (UE) 2016/679 stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor. Printre acestea, se numără cel privind prelucrarea datelor adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (principiul proporționalității), 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) și 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.

Totodată, s-a subliniat că aceleași dispoziții legale sus-menționate prevăd faptul că operatorul este responsabil de respectarea acestor principii şi poate demonstra această respectare (principiul responsabilității).

În ceea ce privește responsabilitatea operatorului, s-a menționat că 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 același timp, s-a precizat că, potrivit prevederilor art. 6 alin. (1) din Legea nr. 176/2010 privind integritatea în exercitarea funcțiilor şi demnităților publice, pentru modificarea şi completarea Legii nr. 144/2007 privind înființarea, organizarea și funcționarea Agenției Naționale de Integritate, precum şi pentru modificarea şi completarea altor acte normative, ”Persoanele responsabile cu implementarea prevederilor referitoare la declaraţiile de avere şi declaraţiile de interese au obligaţia să se înregistreze în această calitate pe e-DAI şi au următoarele atribuţii: (…) d) asigură afişarea şi menţinerea declaraţiilor de avere şi ale declaraţiilor de interese, prevăzute în anexele nr. 1 şi 2, pe pagina de internet a instituţiei, în termen de cel mult 30 de zile de la primire, prin anonimizarea adresei imobilelor declarate, cu excepţia localităţii unde sunt situate, adresei instituţiei care administrează activele financiare, a codului numeric personal, precum şi a semnăturii olografe. Declaraţiile de avere şi declaraţiile de interese se păstrează pe pagina de internet a instituţiei şi a Agenţiei pe toată durata exercitării funcţiei sau mandatului şi 3 ani după încetarea acestora şi se arhivează potrivit legii.”

În același timp, s-a subliniat că, în contextul prelucrării datelor personale, revine operatorilor obligația de analizare și respectare a reglementărilor legale specifice din domeniul propriu de activitate, a Regulamentului (UE) 2016/679, a Legii nr. 190/2018 și a celorlalte reglementări din domeniul protecției datelor, cu respectarea principiilor de prelucrare a datelor statuate de art. 5 din Regulamentul (UE) 2016/679, a tuturor drepturilor persoanelor vizate (prevăzute de art. 12-22 din Regulamentul (UE) 2016/679), precum și cu luarea tuturor măsurilor pentru asigurarea confidențialității și securității datelor.

♦ Furnizarea de imagini din sistemul de supraveghere video al asociației de proprietari

O asociație de proprietari a solicitat un punct de vedere cu privire la legalitatea furnizării imaginilor din sistemul de supraveghere video al asociației de proprietari la solicitarea unui proprietar.

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 video-audio şi stocare a imaginilor şi datelor se supune atât prevederilor Regulamentului (UE) 2016/679, cât şi ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată.

În acest context, Autoritatea națională de supraveghere a menționat că art. 15 din Regulamentul 2016/679, prevede că ”persoana vizată are dreptul de a obţine din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc şi, în caz afirmativ, acces la datele respective şi la următoarele informaţii:

a) scopurile prelucrării;

b) categoriile de date cu caracter personal vizate;

c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din ţări terţe sau organizaţii internaţionale;

d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

e) existenţa dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

f) dreptul de a depune o plângere în fața unei autorităţi de supraveghere;

g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informaţii disponibile privind sursa acestora;

h) existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la articolul 22 alineatele (1) şi (4), precum şi, cel puţin în cazurile respective,

informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată."

Totodată, potrivit alin. (3) al aceluiași articol "Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. (...) În cazul în care persoana vizată introduce cererea în format electronic şi cu excepţia cazului în care persoana vizată solicită un alt format, informaţiile sunt furnizate într-un format electronic utilizat în mod curent."

De asemenea, alin. (4) al art. 15 stipulează că "Dreptul de a obţine o copie menţionată la alineatul (3) nu aduce atingere drepturilor şi libertăţilor altora".

De asemenea, s-a arătat că, în măsura în care o persoană vizată se adresează unui operator de date cu o solicitare prin care își exercită, potrivit art. 15 din Regulamentul (UE) 2016/679, dreptul de acces, operatorul este obligat să îi furnizeze inclusiv o copie a datelor cu caracter personal care fac obiectul prelucrării.

Instituția noastră a mai menționat că, în „Ghidul privind prelucrările de date cu caracter personal efectuate de către asociațiile de proprietari", emis de Autoritatea națională de supraveghere, se arată faptul că operatorul trebuie să acționeze cu prudență și diligență pentru a asigura principiul confidențialității datelor încă de la început și să se asigure că datele personale sunt prelucrate la cel mai înalt nivel de protecție, prin punerea în practică a unor garanții suplimentare precum utilizarea tehnicilor de anonimizare sau de agregare a datelor.

În concluzie, raportat la aspectele mai sus menționate și la necesitatea respectării efective a dreptului la viață privată și la protecția datelor cu caracter personal ale tuturor persoanelor implicate, instituția noastră a precizat că accesul la imaginile din sistemul de supraveghere video se realizează prin anonimizarea datelor cu caracter personal ale celorlalți membri ai asociației de proprietari.

♦ Aplicarea Regulamentului (UE) 2016/679 în procedura de comunicare prin publicitate

O persoana fizică a solicitat un punct de vedere cu privire la legalitatea procedurii de comunicare prin publicitate practicată de instituțiile statului.

Față de această solicitare, Autoritatea națională de supraveghere a făcut următoarele precizări:

Potrivit art. 4 pct. 12 din Regulamentul (UE) 2016/679, „încălcarea securităţii datelor cu caracter personal înseamnă o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea”.

Totodată, s-a menționat că, în ceea ce privește condițiile de legitimitate în care pot fi prelucrate (inclusiv dezvăluite) datele care nu au un caracter special, Regulamentul (UE) nr. 2016/679 prevede la art. 6. alin. (1), prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre condițiile prevăzute la acest articol.

Prin urmare, raportat la prevederile de mai sus, s-a comunicat că datele cu caracter personal pot fi prelucrate (inclusiv dezvăluite) de operatorii de date cu caracter personal cu consimțământul persoanelor vizate sau dacă este îndeplinită una dintre celelalte condiții prevăzute de art. 6 alin. (1) din Regulamentul (UE) 2016/679, cum ar fi îndeplinirea unei obligații legale care îi revine operatorului.

În acest context, s-a precizat că art. 47 din Codul de procedură fiscală prevede următoarele:

„(1) Actul administrativ fiscal trebuie comunicat contribuabilului/plătitorului căruia îi este destinat. În situaţia contribuabilului/plătitorului fără domiciliu fiscal în România, care şi-a desemnat împuternicit potrivit art. 18 alin. (4), precum şi în situaţia numirii unui curator fiscal, în condiţiile art. 19, actul administrativ fiscal se comunică împuternicitului sau curatorului, după caz.

(2) Actul administrativ fiscal emis pe suport hârtie poate fi comunicat fie prin poştă potrivit alin. (3)-(7), fie prin remitere la domiciliul fiscal al contribuabilului/plătitorului ori împuternicitului sau curatorului acestuia potrivit alin. (8)-(12), fie prin remitere la sediul organului fiscal potrivit alin. (13), iar actul administrativ fiscal emis în formă electronică se comunică prin mijloace electronice de transmitere la distanţă potrivit alin. (15)-(17).

(3) Actul administrativ fiscal emis pe suport hârtie se comunică contribuabilului/plătitorului ori împuternicitului sau curatorului acestora, la domiciliul fiscal, prin poştă, cu scrisoare recomandată cu confirmare de primire.

(4) În cazul în care comunicarea potrivit alin. (3) nu a fost posibilă, aceasta se realizează prin publicitate potrivit alin. (5)-(7).

(5) Comunicarea prin publicitate se efectuează prin afişarea unui anunţ în care se menţionează că a fost emis actul administrativ fiscal pe numele contribuabilului/plătitorului, după cum urmează:

a) în cazul actelor administrative fiscale emise de organul fiscal central prin afişarea anunţului, concomitent, la sediul organului fiscal emitent şi pe pagina de internet a A.N.A.F.;

b) în cazul actelor administrative fiscale emise de organul fiscal local prin afişarea anunţului, concomitent, la sediul organului fiscal emitent şi pe pagina de internet a autorităţii administraţiei publice locale respective.

(6) Anunţul prevăzut la alin. (5) se menţine afişat cel puţin 60 de zile de la data publicării acestuia şi conţine următoarele elemente:

a) numele şi prenumele sau denumirea contribuabilului/plătitorului;

b) domiciliul fiscal al contribuabilului/plătitorului;

c) denumirea, numărul şi data emiterii actului administrativ fiscal.

(7) În cazul în care actul administrativ fiscal se comunică prin publicitate, acesta se consideră comunicat în termen de 15 zile de la data afişării anunţului."

Totodată, Autoritatea națională de supraveghere a subliniat faptul că, în contextul analizării constituționalității art. 44 alin. (3) din OG nr. 92/2003 privind Codul de procedură fiscală, Curtea Constituțională a reținut în jurisprudența sa anterioară (Decizia nr. 667/2009, nr. 891/2010, nr. 1387/2010), că dispoziţiile referitoare la comunicarea prin publicitate prin afișare reglementează doar o modalitate ultimă şi subsidiară de comunicare a actelor administrative fiscale, folosită doar în cazul în care celelalte modalităţi de comunicare nu au putut fi îndeplinite din motive obiective.

- ***Legalitatea instalării unui sistem de supraveghere audio-video în secția de anestezie și terapie intensivă***

O unitate medicală a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la legalitatea instalării unor camere de supraveghere video-audio în secția de anestezie și terapie intensivă (ATI).

În acest context, Autoritatea națională de supraveghere a precizat următoarele:

Regulamentul (UE) 2016/679 stabilește că prelucrarea datelor cu caracter personal se realizează cu 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.

Având în vedere solicitarea spitalului, instituția noastră a prezentat existența a două situații pe care operatorul trebuie să le ia în considerare în cazul montării camerelor de supraveghere, raportat la prelucrarea datelor pacienților și ale personalului operatorului.

Pe de o parte, operatorul a fost informat că, în ceea ce privește prelucrarea datelor privind starea de sănătate, această prelucrare se supune prevederilor art. 9 din Regulamentul (UE) 2016/679. Astfel, prelucrarea acestei categorii de date cu caracter special se poate efectua cu respectarea următoarele condiții:

”a) 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; (...)

c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul; (...)

h) prelucrarea este necesară în scopuri legate de medicină preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3);

i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional;(...)”

În acest context, Autoritatea națională de supraveghere a subliniat că, raportat la prelucrările de date preconizate, este necesară analizarea de către fiecare operator a

temeiului legal al efectuării acestora pentru a se asigura conformitate cu dispozițiile Regulamentului (UE) 2016/679, raportat și la reglementările specifice domeniului sănătății.

Astfel, în ceea ce privește datele pacienților, s-a precizat că trebuie ținut cont, în plus, și de reglementările din domeniul sănătății, în mod special de Legea nr. 95/2006 privind reforma în domeniul sănătății, cu modificările și completările ulterioare, precum și de Legea drepturilor pacientului nr. 46/2003, cu modificările și completările ulterioare.

Pe de altă parte, referitor la supravegherea angajaților la locul de muncă prin mijloace de supraveghere video, Autoritatea națională de supraveghere a subliniat și dispozițiile art. 5 din Legea nr. 190/2018 cu privire la condițiile de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă.

Totodată, s-a evidențiat obligația operatorului de informare a persoanelor vizate (ex: angajați, pacienți) și a condițiilor pe care trebuie să le întrunească această informare a prelucrărilor de date efectuate prin intermediul sistemului de supraveghere video.

Astfel, s-a menționat că monitorizarea trebuie precedată de o informare concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Informaţiile se furnizează în scris sau prin alte mijloace și, atunci când este oportun, în format electronic.

În același timp, i s-a comunicat operatorului faptul că, în spaţiile monitorizate trebuie instalată o pictogramă adecvată, care să conţină o imagine reprezentativă, poziţionată la o distanţă rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană.

De asemenea, s-a precizat că, potrivit dispozițiilor art. 12 din Regulamentul (UE) 2016/679, operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul articolelor 15-22 și furnizează acesteia informaţii privind acţiunile întreprinse în urma unei cereri în temeiul acestor articole, fără întârzieri nejustificate şi în orice caz în cel mult o lună de la primirea cererii.

În concluzie, Autoritatea națională de supraveghere a subliniat că monitorizarea prin mijloace video a persoanelor vizate, inclusiv a pacienților și angajaților, nu poate avea loc decât cu respectarea condițiilor legale mai sus amintite.

♦ ***Aplicarea Regulamentului (UE) 2016/679 în contextul autorizării executării lucrărilor de construcții***

O persoană fizică a solicitat Autorității naționale de supraveghere un punct de vedere referitor la aplicarea Regulamentului (UE) 2016/679, în contextul autorizării executării lucrărilor de construcții.

Față de conţinutul solicitării, Autoritatea națională de supraveghere a subliniat următoarele aspecte:

Potrivit Regulamentului general privind protecția datelor, prelucrarea datelor cu caracter personal, inclusiv sub aspectul dezvăluirii acestora, se realizează la consimțământul persoanei vizate sau în celelalte situații prevăzute de art. 6, art. 9 și art. 10 din Regulamentul (UE) 2016/679, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

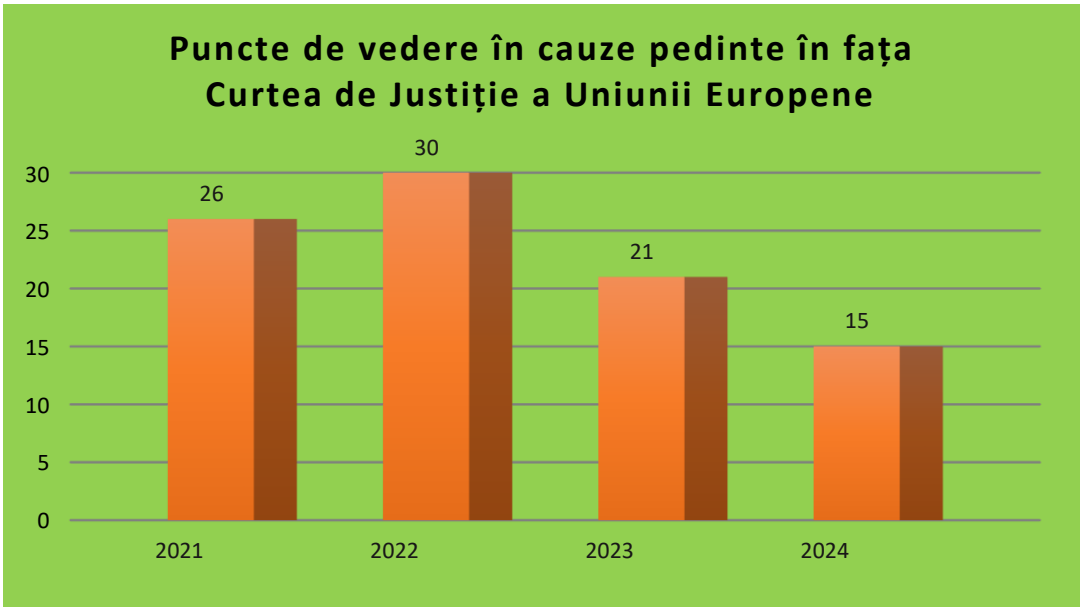
Prin urmare, s-a precizat că, în măsura în care prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului sau prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul, în actele normative naționale (de ex. Legea nr. 50/1991 privind autorizarea lucrărilor de construcție, republicată, respectiv Normele de aplicare ale acestui act normativ) se pot introduce dispoziţii mai specifice de adaptare a aplicării normelor Regulamentului (UE) 2016/679 în ceea ce priveşte prelucrarea prin definirea unor cerinţe specifice mai precise cu privire la prelucrare şi a altor măsuri de asigurare a unei prelucrări legale şi echitabile.

Prin urmare, s-a precizat că prelucrarea datelor personale se efectuează în temeiul art. 6 alin. (1) lit. c) din Regulamentul (UE) 2016/679, coroborat cu prevederile art. 7 alin. (21) – (23^5) din Legea nr. 50/1991 și art. 5 din Normele Metodologice din 2009 de aplicare a Legii nr. 50/1991 aprobate prin Ordinul nr. 839/2009 emis de Ministerului Dezvoltării Regionale şi Locuinței, referitoare la asigurarea transparenţei procedurii de autorizare, coroborate cu cele din art. 55 din același Ordin.

În ceea ce privește aplicarea legislației specifice în domeniul urbanismului și controlul statului în amenajarea teritoriului, urbanism şi autorizarea executării lucrărilor de construcții, s-a menționat că acestea se exercită de Inspectoratul de Stat în Construcții, potrivit legii.

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

În anul 2024, Autoritatea națională de supraveghere a transmis către Ministerul Afacerilor Externe, puncte de vedere în **15 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, Tratatul privind Funcționarea Uniunii Europene – TFUE), astfel:

- Cauza C-480/24 în cadrul căreia cererea a fost adresată de o instanță din Letonia referitoare la interpretarea dispozițiilor art. 2 alin. (1) și (2) și articolul 11 alineatul (1) literele (a) și (b) din Regulamentul (UE) nr. 269/2014 al Consiliului din 17 martie 2014 privind măsuri restrictive în raport cu acțiunile care subminează sau amenință integritatea teritorială, suveranitatea și independența Ucrainei în corelare cu art. 2 din Regulamentul (UE) 2016/679;

- Cauza C-199/24 în cadrul căreia cererea a fost adresată de o instanță din Suedia, referitoare la interpretarea dispozițiilor 85 alin. (1) și (2) din Regulamentul 2016/679;

- Cauza C-312/24 în cadrul căreia cererea a fost adresată de o instanță din Bulgaria, referitoare la interpretarea dispozițiilor art. 2 alin. (1) din Regulamentul 2016/679;
- Cauza C-414/24 în cadrul căreia cererea a fost adresată de o instanță din Austria, referitoare la interpretarea dispozițiilor art. 77 din Regulamentul 2016/679;
- Cauza C-468/24, în cadrul căreia cererea a fost adresată de o instanță din Austria referitoare la interpretarea dispozițiilor art. 5 alin. (3) din Directiva 2002/58 și art. 5 alin. (1) lit. f), art. 13 și art. 32 alin. (2) din Regulamentul (UE) 2016/679;
- Cauza C-474/24 în cadrul căreia cererea a fost adresată de o instanță din Austria referitoare la interpretarea dispozițiilor 16 alin. (2) prima teză din TFUE, art. 5 alin. (1) lit. a) și c), art. 9, art. 6 alin. (3), art. 10 și art. 77 din Regulamentul (UE) 2016/679;
- Cauza C-654/23 Inteligo Media în cadrul căreia cererea a fost adresată de o instanță din România (Curtea de Apel București), referitoare la interpretarea dispozițiilor art. 13 alin. (1) și (2) și art. 15 alin. (2) din Directiva 2002/58/CE și art. 2 lit. f) din Directiva nr. 2000/31/CE raportat la art. 6 alin. (1) lit. a) - f), art. 83 și 95 din Regulamentul (UE) 2016/679;
- Cauza C-371/24 în cadrul căreia cererea a fost adresată de o instanță din Franța referitoare la interpretarea dispozițiilor art. 4 alin. (1) lit. a) - c), raportat la, art. 8 alin. (2) și art. 10 din Directiva nr. 680/2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;
- Cauza C-541/24 în cadrul căreia cererea a fost adresată de o instanță din Bulgaria referitoare la interpretarea dispozițiilor art. 47 coroborat cu art. 7 și 8 din Carta Drepturilor Fundamentale a Uniunii Europene, respectiv art. 19 din Tratatul privind Funcționarea Uniunii Europene și art. 6 alin. (1) lit. a) din Regulamentul (UE) 2016/679;
- Cauza C-526/24 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la interpretarea dispozițiilor art. 12 alin. (5) a doua teză, art. 4 pct. 2 și 82 alin. (1) din Regulamentul (UE) 2016/679;

- Cauza C-484/24 în cadrul căreia cererea a fost adresată de o instanță din Germania referitoare la prelucrarea datelor cu caracter personal ”realizată de o instanță în exercițiul funcției judiciare”;
- Cauza C-422/24 în cadrul căreia cererea a fost adresată de o instanță din Suedia referitoare la interpretarea dispozițiilor art. 13 și art. 14 din Regulamentul (UE) 2016/679.

■ Puncte de vedere exprimate în contextul analizării evaluărilor de impact

- Asociația Română a Băncilor (ARB) a transmis Autorității naționale de supraveghere, spre analiză, ”Evaluarea impactului asupra protecției datelor” pentru prelucrări de date cu caracter personal ce urmau a fi efectuate în contextul serviciului RoPay.

Serviciul RoPay a fost propus de Asociația Română a Băncilor și Transfond ca o soluție care simplifică și securizează procesul de inițiere al plății/al unei solicitări de plată, prin implementarea unui sistem bazat pe o platformă centrală Mobile Platform System („MPS” sau „Platforma”) administrată de Transfond și pe aplicațiile de mobile/internet banking ale unor instituții de credit, instituții emitente de monedă electronică sau instituții de plată, utilizând numărul de telefon ca identificator unic al persoanei fizice care urmează să facă plata ("plătitor”) sau a celei care urmează să încaseze fondurile ("beneficiar”), în funcție de serviciul accesat.

În vederea implementării acestei scheme de plăți urmau a fi efectuate o multitudine de prelucrări de date cu caracter personal care implicau anumite riscuri cu privire la datele clienților băncilor, persoane fizice, din postura acestora de beneficiari ai plăților, precum și de plătitori, aspecte complexe privind prelucrările de date cu caracter personal legate de serviciul RoPay.

Documentul ”Evaluarea impactului asupra protecției datelor” pentru prelucrările de date cu caracter personal efectuate în contextul serviciul RoPay, a fost analizat la nivelul Autorității naționale de supraveghere prin raportare la dispozițiile Regulamentului (UE) 2016/679 și a celorlalte reglementări aplicabile, și ulterior a fost modificat și completat,

inclusiv ca urmare a discuțiilor dintre reprezentanții Asociației Române a Băncilor, Băncii Naționale a României, Transfond și cei ai Autorității naționale de supraveghere.

- Un spital județean de urgență a transmis Autorității naționale de supraveghere, spre analiză, ”Evaluarea de impact privind protecția datelor cu caracter personal pentru sistemul de supraveghere video”.

Instalarea sistemului de supraveghere video în serviciul UPU-SMURD ar fi avut ca scop prevenirea incidentelor (infracțiuni, comportament neadecvat), imaginile video urmând a fi folosite ca probe de către organele abilitate.

În urma analizării documentului mai sus menționat, Autoritatea națională de supraveghere a apreciat că evaluarea de impact privind protecția datelor cu caracter personal pentru sistemul de supraveghere video în serviciul UPU-SMURD realizată de spitalul respectiv, nu întrunește condițiile unei evaluări de impact, raportat la dispozițiile Regulamentului (UE) 2016/679.

- Un penitenciar a transmis Autorității naționale de supraveghere, spre analiză „evaluarea de impact asupra protecției datelor cu caracter personal în privința introducerii în sistemul de monitorizare video a unor camere cu opțiunea de recunoaștere pe bază de imagini faciale”.

Prin instalarea camerelor de supraveghere video cu opțiunea de recunoaștere pe bază de imagini faciale, penitenciarul intenționa să realizeze paza obiectivului numai prin intermediul sistemului de supraveghere video, eliminând astfel personalul din posturile respective, acesta putând desfășura alte activități.

Urmare a analizării evaluării de impact, raportat la activitățile desfășurate de instituția mai sus menționată, operatorului i s-a adus la cunoștință că prelucrările de date pe care le efectuează se supun și prevederilor Legii nr. 363/2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date.

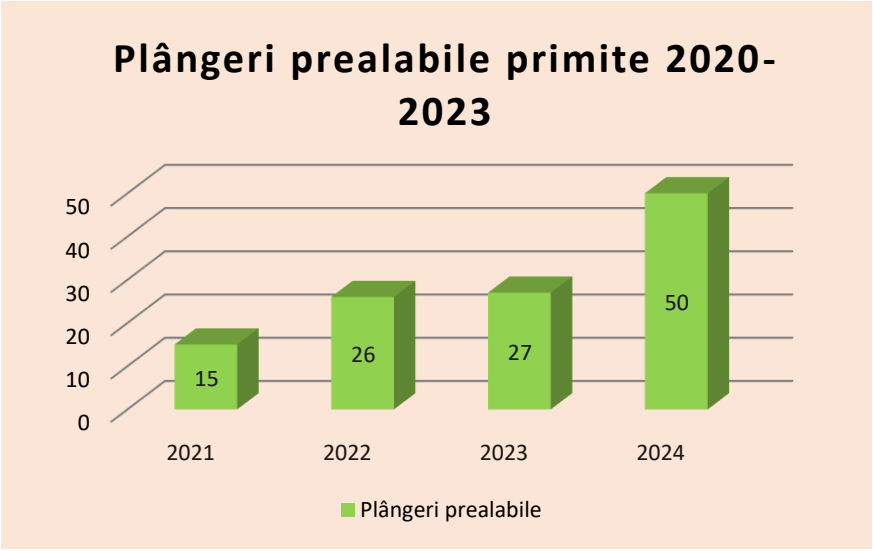
Astfel, Autoritatea națională de supraveghere a apreciat că evaluarea de impact stabilită de operatorul sus menționat trebuie realizată potrivit dispozițiilor Regulamentului (UE) 2016/679, respectiv Legii nr. 363/2018, prin raportare la natura datelor cu caracter personal prelucrate, domeniul de aplicare, contextul şi scopurile prelucrării.

■ 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 2024,** au fost depuse la Autoritatea națională de supraveghere un număr de **50 plângeri prealabile**.

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



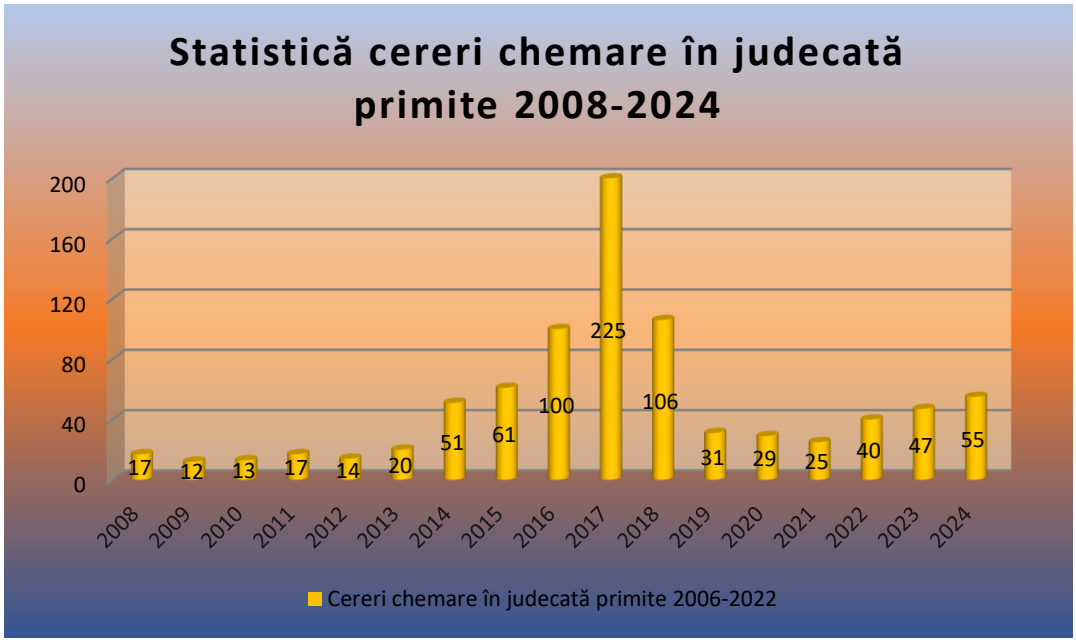
Secțiunea a 3 - a
Activitatea de reprezentare în fața instanțelor de judecată

În anul 2024, Autoritatea națională de supraveghere a gestionat un număr de 173 dosare aflate pe rolul instanțelor de judecată în diferite stadii procesuale.

Dintre acestea, **pe parcursul anului 2024** 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, **16 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 2019-2024, au fost până în prezent definitivate 47 dosare, iar dintre acestea în 40 de cauze au fost pronunțate soluții definitive în favoarea Autorității naţionale de supraveghere.



În anul 2024 au fost finalizate definitiv mai multe acțiuni în mod favorabil pentru instituția noastră, dintre care prezentăm mai jos câteva **cazuri 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 transmiterii de către operator a unei notificări de încălcare a securității datelor cu caracter personal, în temeiul Regulamentului (UE) nr. 679/2016.

În cadrul investigației efectuate s-a constatat faptul că încălcarea securității prelucrării datelor s-a produs prin accesarea neautorizată a infrastructurii informatice gestionate de către operator, ceea ce a făcut posibilă descărcarea și ștergerea anumitor date cu caracter personal.

Această situație a condus la divulgarea neautorizată sau accesul neautorizat la anumite date cu caracter personal din CV-urile candidaților**,** cum sunt: nume, prenume, e-mail, număr de telefon, istoric profesional/educațional, hobby-uri, stare familială.

Astfel, operatorul a fost sancționat cu amendă în cuantum de 24.610 lei, echivalentul a 5.000 EURO pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) nr. 679/2016, întrucât nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării.

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

Tribunalul Cluj a dispus înlocuirea amenzii în cuantum de 24.610 lei (echivalentul a 5.000 euro) cu sancțiunea avertismentului.

Dar Curtea de Apel Cluj a admis apelul formulat de Autoritatea naţională de supraveghere, a schimbat în tot sentinţa apelată și a respins cererea de chemare în judecată a operatorului.

Prin hotărârea dată, instanța de apel a reținut că *"amenda în cuantum de 24.610,5 lei respect principiul proporționalității, fiind aplicată în acord cu criteriile menționate la art. 83 alin. (2) din Regulament, neimpunându-se înlocuirea acesteia cu sancțiunea contravențională a avertismentului."*

De asemenea, Curtea de Apel Cluj a reținut că *„incidentul de securitate nu a fost descoperit de către intimată printr-o verificare proprie, ci aceasta a fost sesizată de un colaborator, care a informat CEO-ul companiei, aspect care denotă o disfuncție în implementarea măsurilor tehnice organizatorice adecvate riscului.”*

Hotărârea judecătorească, favorabilă Autorității naționale de supraveghere, a rămas definitivă.

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea prevederilor art. 32 alin. (1) lit. b), alin. (2) și alin. (4) din Regulamentul (UE) nr. 679/2016**

Autoritatea națională de supraveghere a efectuat o investigaţie ca urmare a transmiterii de către operator a unei notificări de încălcăre a securității datelor cu caracter personal în temeiul Regulamentului (UE) nr. 679/2016.

În cadrul investigației efectuate s-a constatat faptul că încălcarea securității prelucrării datelor s-a produs prin utilizarea incorectă a funcției de tipărire în sistemul informatic utilizat pentru gestionarea facturilor, ceea ce a condus la emiterea în mod eronat a datelor de facturare și generarea unui număr foarte mare de facturi, precum și afișarea acestora pe portalul operatorului, fiind afectate un număr mare de persoane fizice ale căror date cu caracter personal: nume, prenume, adresă, cod încasare, cod client, cod loc de consum, număr de contract, sold, date consum, au fost dezvăluite.

Prin urmare, operatorul a fost sancționat cu amendă în cuantum de 24.861 RON (echivalentul a 5.000 EURO), pentru încălcarea 32 alin. (1) lit. b), alin. (2) și alin. (4) din Regulamentul (UE) nr. 679/2016.

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

Tribunalul Mureș a reținut că *„reclamanta nu a reuşit să facă proba contrară care îi incumbă sub aspectul temeiniciei actului constatator, din contră, prin precizările formulate aceasta recunoaşte indirect săvârşirea faptei contravenţionale. Producerea incidentului care, astfel cum sustine reclamanta, s-a datorat unei erori umane cauzată de utilizarea neconformă cu instrucţiunile de lucru a functionalităţii de tipărire manuală a facturilor,*

denotă că reclamanta nu a luat şi nu a implementat toate măsurile tehnice şi organizatorice necesare asigurării unui nivel corespunzător de securitate al datelor personale."

De asemenea, în mod corect a reținut instanța de fond și faptul că *„în cauza de faţă sancţiunea amenzii aplicată acesteia şi care reprezintă echivalentul în lei a sumei 5000 euro, a fost in mod corect individualizată de pârâtă, iar tribunalul nu are motive pentru a proceda la o reindividualizare a sancţiunii aplicate.*

Astfel se constată că în cauză limita maximă a amenzii este de 10.000.000 euro, iar faţă de împrejurările în care a fost săvarşită fapta, modul şi mijloacele de săvarşire a acesteia, de scopul urmărit la edictarea normei încălcate şi de urmarea produsă, care a constat în dezvăluirea datelor personale ale unui număr de 714 persoane fizice, nu se impune nici reducerea cuantumului amenzii aplicate şi nici înlocuirea acesteia cu sancţiunea avertismentului."

Prin hotărârea dată, instanța de apel a reținut că *„Referitor la temeinicia procesului verbal şi individualizarea sancțiunii aplicate, Curtea va considera ca judicioase aspectele reținute de către instanţa de fond. În cuprinsul probatoriului administrat în cauză este evidentă neîndeplinirea de către reclamanta-apelantă a obligaţiilor de diligență și de rezultat pe care le avea, rezultatul fiind unul cu impact semnificativ în ceea ce priveşte protecția datelor cu caracter personal ale clienților. Producerea incidentului de securitate semnificativ este revelator în această privinţă, iar atitudinea reclamantei de anunţare a organului competent nu poate avea semnificaţia unei culpe scăzute, ci reprezintă doar conformarea la conduita impusă de normele legale aplicabile."*

Totodată, Curtea de Apel Târgu Mureș a constatat cu privire la individualizarea sancțiunii contravenționale că *„aceasta a avut în vedere tocmai conduita ulterioară a reclamantei şi încercarea acesteia de a limita efectele incidentului de securitate, acesta fiind şi motivul pentru care amenda este orientată către minimul prevăzut de lege"* și că *„în acord cu soluţia primei instanțe, nu se impune înlocuirea sancţiunii amenzii cu cea a avertismentului sau aplicarea minimului amenzii."*

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

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea prevederilor art. 5, art. 6, art. 9, art. 17 și art. 32 alin. (1) și (2) din Regulamentul (UE) nr. 679/2016**

Autoritatea națională de supraveghere a efectuat o investigație ca urmare a unei plângeri prin care s-a reclamat divulgarea de către operator a datelor personale ale unui client (persoană fizică), prin postarea unei înregistrări audio-video pe paginile de socializare ale operatorului.

În cadrul investigației efectuate Autoritatea națională de supraveghere a constatat că operatorul, prin intermediul paginilor sale de socializare, a diseminat datele clientului din înregistrarea audio-video și a folosit în comentarii un apelativ ce dezvăluia originea etnică a acestuia, fără a avea temei legal, încălcându-se astfel prevederile art. 5, 6 și 9 din Regulamentul (UE) 2016/679.

De asemenea, s-a constatat că operatorul nu a dat curs cererii clientului de ștergere a datelor, încălcând prevederile art. 17 din Regulamentul (UE) 2016/679.

În același timp, s-a constatat și faptul că operatorul nu a adoptat suficiente măsuri tehnice și organizatorice adecvate în vederea asigurării confidențialității datelor personale prelucrate prin intermediul sistemului de supraveghere audio-video.

Prin urmare, operatorul a fost sancționat contravențional cu amenzi în cuantum total de 49.322 lei (echivalentul a 10.000 Euro), pentru încălcarea prevederilor art. 5, 6, 9, 17 și art. 32 alin. (1) și (2) din Regulamentul (UE) 2016/679. Totodată, în sarcina operatorului s-au dispus și anumite măsuri corective.

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

Prin decizie definitivă, Curtea de Apel Iași a confirmat abordarea Autorității naționale de supraveghere și a reținut că: *„În cauză prelucrarea unor date cu caracter personal a fost făcută de un operator stabilit în UE (respectiv de către apelantă) și a vizat monitorizarea comportamentului unei persoane care se află în Uniune. În aceste condiții, așa cum corect a reținut și prima instanță, dispozițiile Regulamentului (UE) 2016/679 sunt aplicabile în cauză."*

De asemenea, în ceea ce privește modalitatea de individualizare a sancțiunii aplicate, în mod corect a reținut instanța de apel că *„apelantei i-a fost aplicată o amendă în cuantum total de 10.000 euro. Or, potrivit art. 83 alin. 5 din regulament amenda pentru fiecare din cele trei contravenții reținute în sarcina apelantei era de până la 4% din cifra de afaceri*

mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare. Cum cifra de afaceri a apelantei, conform celor reținute în cuprinsul procesului verbal este de 3.671.268 lei (...) amenda maximă ce putea fi aplicată era de 146.850,72 lei. Apelantei i-a fost aplicată o amendă totală mult sub maximul prevăzut de regulament, amenda pe deplin justificată prin raportare la gravitatea faptelor imputate, ținând cont și de conduita apelantei."

Ca atare, instanța 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 supraveghere video de către o instituție publică**

Autoritatea națională de supraveghere a efectuat o investigație ca urmare a unei plângeri prin care a fost semnalată o posibilă încălcare a prevederilor legale referitoare la prelucrarea datelor cu caracter personal de către o unitate administrativ-teritorială prin intermediul unor camere de supraveghere video, prin care ar fi fost monitorizați și verificați toți angajații instituției.

În cadrul investigației s-a constatat că operatorul nu a făcut dovada informării persoanelor vizate cu privire la drepturile prevăzute de Regulamentul (UE) 2016/679 și nici a adoptării la nivelul unității administrativ-teritoriale a unor măsuri de securitate și confidențialitate adecvate pentru protecția datelor personale prelucrate prin intermediul sistemului de supraveghere video deținut, fiind încălcate prevederile art. 13, art. 14 și ale art. 32 din Regulamentul (UE) 2016/679.

Operatorul a fost sancționat cu amendă în cuantum de 10.000 lei, pentru faptul că nu a adus la îndeplinire măsurile dispuse anterior de Autoritatea națională de supraveghere printr-un plan de remediere și pentru că nu a răspuns solicitărilor Autorității.

Totodată, operatorul a fost sancționat cu avertisment pentru lipsa informării persoanelor vizate cu privire la drepturile acestora prevăzute de Regulamentul (UE) 2016/679, precum și pentru neadoptarea unor măsuri de securitate și confidențialitate

adecvate pentru protecția datelor personale prelucrate prin intermediul sistemului de supraveghere video.

De asemenea, Autoritatea naţională de supraveghere a aplicat și măsuri de remediere, dispunând operatorului:

- să dea curs tuturor solicitărilor Autorității, așa cum s-a dispus prin planul de remediere;

- să implementeze măsuri de securitate și confidențialitate adecvate în ceea ce privește protecția datelor personale prelucrate prin sistemul de supraveghere video al unității administrativ teritoriale și să transmită Autorității naționale de supraveghere, în copie, procedura/procedurile adoptate și dovezile efectuării instruirii persoanelor care au acces la imaginile preluate prin intermediul sistemului de supraveghere video;

- să ia măsurile necesare astfel încât persoanele vizate să fie informate cu privire la drepturile prevăzute de Regulamentul (UE) 2016/679 în acord cu dispozițiile art. 13 și art. 14 din același Regulament.

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

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

În susținerile sale, instanța de fond a constatat faptul că *"Prin procesul verbal de constatare/sanctionare (...) emis de Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal reclamanta (...) a fost sancţionată pentru fapta prevăzută de art. 12 şi art. 14 alin. 5 lit. e din Legea nr. 190/2018 raportat la dispoziţiile art. 83 alin. 5 lit. e din Regulamentul (UE) 2016/679 (RGPD), la data incheierii procesului verbal, constatându-se că (,,,) nu a dus la îndeplinire măsurile prevăzute in Planul de remediere (...) anexat la procesul verbal (...) in termenul de 6 zile lucrătoare de la data comunicării procesului verbal, şi prin urmare nu a răspuns tuturor solicitărilor autorităţii de supraveghere formulate (...) cuprinse in planul de remediere (...), precum şi solicitărilor aceleiași autorităţi formulate (...)."*

Instanța de fond a reținut că operatorul *"nu a făcut dovada informării persoanelor cu privire la drepturile prevăzute de Regulamentul (UE) 2016/679 şi a adoptării (...) unor măsuri de securitate şi confidenţialitate adecvate pentru protecţia datelor personale prelucrate prin intermediul sistemului de supraveghere video, cu încălcarea prevederilor art. 13 şi art. 14 şi a obligaţiilor impuse de art. 32 din același Regulament."*

Sub aspectul legalității procesului verbal de contravenţie, instanța de fond a reținut că *„acesta a fost încheiat cu respectarea prevederilor art. 17 din O.G. nr. 2/2001 privind regimul juridic al contraventiilor, nefiind incident niciunul din cazurile de nulitate absolută care pot fi invocate şi din oficiu de instanţa de judecată*."

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

Prin hotărârea dată, instanța de apel a reținut în legătură cu operatorul că *„susținerile formulate sunt neîntemeiate, iar hotărârea primei instanțe este pronunțată cu aplicarea corectă a dispozițiilor legale", "motiv pentru care (...) respinge apelul declarat de reclamantă".*

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

- **Hotărâre definitivă pronunțată într-un litigiu privind încălcarea dispozițiilor art. 25 alin. (1), art. 32 alin. (1) lit. b) și d) și art. 32 alin. (2) din Regulamentul (UE) 2016/679**

Autoritatea națională de supraveghere a efectuat o investigație ca urmare a transmiterii de către operator a unei notificări de încălcare a securității datelor cu caracter personal în temeiul Regulamentului (UE) nr. 679/2016.

În cadrul investigației, s-a constatat că încălcarea securității prelucrării datelor s-a produs ca urmare a faptului că operatorul a introdus în secțiunea de plăți online a site-ului pe care îl deține un formular neautorizat prin care se colectau date bancare conținute de cardurile clienților, ceea ce a condus la divulgarea neautorizată și accesul neautorizat la anumite date cu caracter personal, cum ar fi: numele și prenumele deținătorului cardului bancar, numărul cardului, data și anul expirării, cod CVC.

De asemenea, s-a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine

Ca atare, operatorul a fost sancționat contravențional cu amendă în cuantum de 9.883 lei (echivalentul a 2000 EURO).

Operatorul a contestat în instanță procesul–verbal de constatare/sancționare încheiat de Autoritatea Națională de Supraveghere.

Analizând probatoriul administrat în cauză, tribunalul a admis în parte cererea de chemare în judecată formulată de operator și a dispus înlocuirea sancțiunii amenzii cu aceea a avertismentului.

Astfel, Tribunalul Timiș a reținut că *„sancțiunea amenzii în cuantum de 9.883,60 lei, aplicată în cauză, reprezintă o sancțiune prea severă față de conținutul concret al faptei, caracterul izolat al acesteia, lipsa altor abateri ilicite anterioare, împrejurarea că reclamanta şi-a corectat într-un timp foarte scurt şi în mod eficient conduita neconformă prin adoptarea măsurilor adecvate de natură a preîntâmpina situațiile de genul celei consemnate în procesul verbal.*

În activitatea reclamantei, acesta pare a fi primul incident de securitate, unul izolat, pârâta neadministrând probe din care să rezulte contrariul.

De asemenea, mai are in vedere şi conduita reclamantei, faptul că a luat de îndată măsuri tehnice şi organizatorice pentru a soluționa şi a limita consecinţele încălcării securității datelor, a procedat la informarea celor două persoane vizate şi a sesizat imediat organele abilitate, ceea ce denotă înțelegerea pe deplin a valorilor sociale ocrotite de legiuitor. (…)"

Autoritatea națională de supraveghere a formulat apel doar sub aspectul individualizării sancțiunii.

Curtea de Apel Timișoara a menținut sentința primei instanțe.

Hotărârea judecătorească, parțial favorabilă Autorității naționale de supraveghere, a rămas definitivă.

- **Hotărâre definitivă pronunțată într-un litigiu privind utilizarea unui sistem de supraveghere video pentru realizarea pontajului angajaților într-o instituție publică**

Autoritatea națională de supraveghere a efectuat o investigație la o instituție publică, ca urmare a unei sesizări cu privire la o posibilă încălcare a dispoziţiilor Regulamentului (UE)

2016/679, în contextul utilizării înregistrărilor din sistemul de supraveghere video în scopul realizării pontajului angajaților operatorului.

În cadrul acestei investigații s-a constatat faptul că operatorul de date cu caracter personal a încălcat prevederile art. 5 alin. (1) lit. b) și art. 6 din Regulamentul (UE) 2016/679, deoarece a prelucrat date cu caracter personal ale angajaților proprii, respectiv imagini înregistrate/stocate de sistemul de supraveghere video de la nivelul operatorului, într-un alt scop (întocmirea pontajului) decât scopul declarat al prelucrării („paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor”), fără să existe o obligație legală a operatorului și fără îndeplinirea vreunei alte condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679, iar potrivit art. 5 alin. (1) lit. b) din Regulamentul (UE) 2016/679 avea obligația de a colecta date cu caracter personal în scopuri determinate, explicite și legitime și de a nu le prelucra ulterior într-un mod incompatibil cu aceste scopuri.

Autoritatea națională de supraveghere a aplicat sancțiunea avertismentului și, conform art. 13 alin. (1) din Legea nr. 190/2018, la procesul-verbal emis a fost anexat un plan de remediere, prin care s-a dispus ca operatorul să asigure conformitatea cu dispozițiile Regulamentului (UE) 2016/679 a operațiunilor de prelucrare a datelor cu caracter personal, inclusiv a celor efectuate prin intermediul sistemului de supraveghere video, prin implementarea de măsuri tehnice și organizatorice ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor (de ex. proceduri de lucru referitoare la protecția datelor cu caracter personal, precum și măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea sa, referitor la obligațiile ce le revin conform prevederilor Regulamentului (UE) 2016/679 și la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii).

Ulterior, a fost efectuată o nouă investigație, la sediul operatorului, în vederea verificării îndeplinirii măsurilor dispuse anterior prin planul de remediere, iar Autoritatea națională de supraveghere a constatat că operatorul investigat a încălcat prevederile art. 14 alin. (7), coroborat cu art. 14 alin. (1) și art. 13 alin. (4) din Legea nr. 190/2018, deoarece nu a adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere și în termenul de remediere dispus.

Procesul-verbal de constatare/sancționare emis de Autoritatea națională de supraveghere a fost contestat de operatorul sancționat cu amendă în cuantum de 13.000 lei.

Instanța de fond a respins ca vădit neîntemeiată plângerea contravenţională formulată de operator, iar în ceea ce privește fondul cauzei**,** în mod corect, Tribunalul București a reținut în sentința pronunțată, următoarele:

"Prin procesul-verbal de constatare/sancţionare a contravenţiei (...) întocmit de Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal la data de (...), petenta (….) a fost sancționată cu amendă contravenţională în cuantum de 13000 lei pentru săvârșirea contravenției prevăzute de art. 14 alin. (7) coroborat cu art. 14 alin. (1) şi art. 13 alin. (4) din Legea nr. 190/2018 (…), reținându-se în sarcina acesteia că la data încheierii procesului-verbal (...) nu a adus la îndeplinire în totalitate măsurile prevăzute în planul de remediere (...), în termenul de remediere de 20 de zile lucrătoare de la data comunicării procesului-verbal (...)."

Cu privire la legalitatea procesului-verbal de constatare/sancţionare a contravenţiei prin care a fost aplicată amenda de 13.000 lei, Tribunalul București a reținut că:

-"acesta a fost încheiat cu respectarea dispoziţiilor legale incidente, neexistând cazuri de nulitate absolută ce ar putea fi invocate din oficiu de către instanţă."

- "Tribunalul constată că lipsa semnăturii martorului asistent din cuprinsul procesului-verbal de contravenție nu este prevăzută sub sancțiunea nulității absolute. "

-"Tribunalul constată că petenta (…) nu a depus la dosarul cauzei nicio dovadă din care să reiasă că a adus la îndeplinire in totalitate, în termenul de remediere de 20 de zile lucrătoare de la data comunicării procesului-verbal de contravenţie, (...) măsurile prevăzute în planul de remediere"

-" În ceea ce priveşte individualizarea sancţiunii contravenţionale aplicate, respectiv amendă contravenţională în cuantum de 13.000 lei (limita minimă a amenzii fiind de 10.000 lei) pentru săvârșirea contravenţiei prevăzute de art. 14 alin. (7) coroborat cu art. 14 alin. (1) şi art. 13 alin. (4) din Legea nr. 190/2018 (…), instanţa constată legalitatea şi temeinicia acesteia."

- "Tribunalul constată că fapta contravenţională săvârșită de petenta (…) este de o gravitate sporită, ceea ce face absolut necesară sancționarea cu amendă contravenţională a unei asemenea fapte." și că *"(...) scopul educativ, dar şi cel punitiv al sancţiunii contravenţionale poate fi atins numai prin menținerea amenzii contravenționale în cuantum de 13000 lei, aplicate prin procesul-verbal contestat, de natură să corecteze atitudinea petentei, in acest fel asigurându-se atât prevenția generală, cât şi cea specială, ceea ce nu*

se poate realiza in niciun caz prin înlocuirea sancţiunii amenzii contravenţionale in cuantum de 13000 lei, aplicate prin procesul-verbal contestat cu sancţiunea avertismentului.

-"instanţa apreciază că sancţiunea aplicată, respectiv amenda contravenţională în cuantum de 13000 lei a fost în mod just şi legal individualizată, fiind un raport de proporţionalitate cu pericolul social concret al faptei, având în vedere ansamblul împrejurărilor în care a fost comisă de către petentă."

Curtea de Apel București 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 2024, 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 Protecţiei Datelor – 28 Ianuarie 2024

Pe data de 28 ianuarie 2024 se celebrează Ziua Europeană a Protecției Datelor de către toate statele membre ale Consiliului Europei, când s-au împlinit 43 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.

Sărbătorirea anuală a acestei zile se subsumează obiectivului ridicării nivelului de conștientizare a publicului larg cu privire la regulile de utilizare a datelor cu caracter

personal, sub egida evidențierii importanței dreptului la viață privată și la protecția datelor personale.

Pentru celebrarea Zilei Europene a Protecţiei Datelor, instituția noastră a organizat, **pe data de 26 ianuarie 2024**, **Conferința online intitulată „Rolul și eficiența activității responsabilului cu protecția datelor”,** în care au fost prezentate și dezbătute aspecte specifice prelucrării datelor cu caracter personal, în special în ceea ce privește rolul responsabilului cu protecția datelor. La acest eveniment au fost invitate, în principal, autoritățile și instituțiile publice centrale reprezentative, cele mai importante asociații și uniuni profesionale, organizațiilor nonguvernamentale, camere de comerț, companii și reprezentanți mass-media.

Cu acest prilej, au fost aduse atât în atenția operatorilor, cât și a persoanelor împuternicite, aspecte specifice prelucrării datelor cu caracter personal, în special în ceea ce privește rolul responsabilului cu protecția datelor.

De asemenea, ca în fiecare an, 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 Protecţiei Datelor, precum și informații privind activitatea din anul anterior.

Totodată, pentru celebrarea 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.

În același timp, instituția noastră a propus Ministerului Afacerilor Interne și Ministerului Afacerilor Externe, organizarea de manifestări destinate creșterii gradului de informare cu privire la aplicarea specifică a regulilor de protecție a datelor de către personalul polițienesc, respectiv de către personalul diplomatic și consular, inclusiv cu privire la noutățile aduse prin Regulamentele (UE) 2018/1860, 2018/1861, 2018/1862, aplicabile în domeniul Schengen.

♦ **Moment aniversar - șase ani de la aplicarea Regulamentului (UE) 2016/679 – 25 Mai 2024**

Cu prilejul sărbătoririi a șase ani de la aplicarea Regulamentului (UE) 2016/679, a fost postat pe site-ul instituției un comunicat de presă ce prezintă o sinteză a celor mai

semnificative aspecte din activitatea Autorității naţionale de supraveghere, desfășurată pe parcursul primelor patru luni ale anului 2024, aspect ce relevă faptul că s-a continuat activitatea de monitorizare și control cu privire la legalitatea prelucrărilor de date personale.

În cinstea acestui prilej aniversar, în perioada 23 - 24 mai 2024, instituția noastră a inițiat și a organizat reuniuni de pregătire în domeniul protecției datelor cu caracter personal a personalului Ministerului Afacerilor Externe, organizate cu sprijinul acestui minister la Centrul de Instruire a Personalului Consular.

♦ **Acțiuni de informare destinate popularizării regulilor de protecție a datelor cu caracter personal**

Autoritatea națională de supraveghere a continuat și anul acesta activităţile de comunicare destinate informării publicului larg, cu privire la regulile de prelucrare a datelor cu caracter personal, raportat la competențele sale stabilite prin Regulamentul General privind Protecţia Datelor, în scopul creșterii nivelului de înțelegere în rândul publicului larg a riscurilor, regulilor şi drepturilor în domeniul datelor cu caracter personal.

În acest context, menționăm că instituția noastră a propus Ministerului Afacerilor Interne și Ministerului Afacerilor Externe, organizarea de manifestări destinate creșterii gradului de informare cu privire la aplicarea specifică a regulilor de protecție a datelor de către personalul polițienesc, respectiv de către personalul diplomatic și consular, inclusiv cu privire la noutățile aduse prin Regulamentele (UE) 2018/1860, 2018/1861, 2018/1862, aplicabile în domeniul Schengen.

Astfel, în perioada 04 - 07 noiembrie 2024, Autoritatea națională de supraveghere a susținut patru sesiuni de pregătire a personalului Poliției de Frontieră, în domeniul protecției datelor, în contextul aderării țării noastre la Schengen aerian și maritim.

În cadrul acestor seminare organizate de Inspectoratul General al Poliției de Frontieră, la inițiativa instituției noastre, au fost prezentate informații privind statutul și competențele Autorității naţionale de supraveghere, principalele reguli de prelucrare a datelor personale statuate de Legea nr. 363/2018, raportat la specificul activității polițiștilor de frontieră. S-a evidențiat importanța realizării informării cu privire la drepturile persoanelor vizate la punctele de trecere a frontierelor, în concordanță cu prevederile legale aplicabile.

În același timp, au fost prezentate aspecte relevante privind asigurarea confidențialității și securității prelucrărilor de date și exemple practice din activitatea de control în domeniul protecției datelor.

♦ **Conferințe, seminare, reuniuni**

Instituţia noastră a participat activ și în anul 2024 la **reuniuni** 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 anumite aspecte privind condițiile utilizării datelor, respectarea drepturilor persoanelor vizate, asigurarea confidenţialităţii și protecției datelor cu caracter personal, ceea ce reflectă continuitatea deschiderii către societatea civilă.

Astfel, menționăm că, în data de 14 martie 2024, reprezentanții Autorității naționale de supraveghere au susținut la Ploiești „Cursul în domeniul protecției datelor cu caracter personal", destinat responsabililor cu protecția datelor desemnați la nivelul structurilor subordonate ale Ministerului Afacerilor Interne.

Cursanții au reprezentat structuri din cadrul Ministerului Afacerilor Interne precum Jandarmeria Română, Inspectoratul General al Poliției de Frontieră, Inspectoratul General pentru Imigrări, Inspectoratul pentru Situații de Urgență, etc.

În cadrul cursului structurat pe două module, "Drepturile persoanelor vizate în contextul prelucrării datelor cu caracter personal", respectiv "Organizarea și funcţionarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Național", au fost prezentate aspecte cu caracter general și specific precum drepturile persoanelor vizate și atribuţiile de supraveghere și control ale Autorității naționale de supraveghere, raportat la dispozițiile Regulamentului (UE) 2016/679 și la prevederile Legii nr. 363/2018.

Cu acest prilej, au fost supuse dezbaterii inclusiv aspecte practice referitoare la aplicarea legislaţiei protecției datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date, precum și aspecte specifice privind acquis-ul Schengen și aplicarea acestuia.

Reprezentanții Autorității naționale de supraveghere au adus în atenția participanților faptul că fiecărui operator îi revine obligația de a identifica în mod corect temeiurile legale de prelucrare raportat la activitățile desfășurate, de a efectua evaluări în urma instruirii

angajaților cu privire la prelucrarea datelor, de a face evaluări de impact atunci când se impune, de a realiza o informare completă a persoanelor vizate, potrivit Regulamentului (UE) 2016/679 sau Legii nr. 363/2018, în funcție de fiecare situație specifică apărută la nivelul structurilor Ministerului Afacerilor Interne, precum și de a stabili măsuri de confidențialitate și securitate specifice pentru prelucrările de date efectuate de fiecare structură în parte.

De asemenea, 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, cum ar fi:**

- Biroul Român de Audit Transmedia (BRAT) - discuții referitoare la implementarea butoanelor ”Accept toate” și ”Vreau să modific setările individual” în primul ecran al site-urilor aparținând publisher-ilor (editori) din România care utilizează platforma standardizată de management al consimțământului - SATI-PMC pentru gestionarea opțiunilor exprimate de către utilizatori, cu privire la folosirea tehnologiilor de tip cookie, raportat la prevederile art. 4 alin. (5) din Legea nr. 506/2004, privind consimțământul.

Autoritatea națională de supraveghere a recomandat completarea informării persoanelor vizate, ce se regăsește, de asemenea, în primul ecran, cu o mențiune în sensul că în această primă etapă nu sunt plasate cookie-uri, altele decât cele strict necesare pentru funcționarea site-urilor/aplicațiilor editorilor și pentru furnizarea serviciilor (raportat la art. 4 alin. (6) lit. b) din Legea nr. 506/2004).

- Asociația Română a Băncilor, Banca Națională a României și Transfond – discuții referitoare la implementarea serviciul RoPay.

- Consiliul Superior al Magistraturii - în considerarea excelentei colaborări interinstituționale cu Consiliul Superior al Magistraturii și a noilor evoluții legislative privind desemnarea Consiliului ca autoritate competentă pentru supravegherea operaţiunilor de prelucrare a datelor cu caracter personal de către instanţele judecătoreşti, în exercitarea atribuţiilor lor judiciare, potrivit prevederilor art. 34 alin. (2) din Legea nr. 305/2022, în data de 22 aprilie 2024 a avut loc o întrevedere între reprezentanții Autorității naționale de supraveghere și cei ai Consiliului la nivelul căruia s-a constituit grupul de lucru care să elaboreze un Cod de Conduită ce ar urma să fie aplicat de către instanțele de judecată.

- Asociația de Management al Creanțelor Comerciale (AMCC) – discuții referitoare la aspecte operaționale ce țin de activitatea curentă a companiilor ce activează în domeniul colectării de creanțe comerciale în corelare cu aspecte ce țin de aplicabilitatea Ordonanței de

Urgență a Guvernului nr. 15/2024 privind administratorii de credite și cumpărătorii de credite, precum și pentru modificarea și completarea unor acte normative privind contractele de credit pentru consumatori.

- Consiliul Concurenței - discuții privind cooperarea dintre Consiliu Concurenței și Autoritatea națională de supraveghere.

- Departamentul pentru Lupta Antifraudă (DLAF) - discuție cu privire la aspecte privind prelucrări de date efectuate la nivelul Departamentului pentru Lupta antifraudă.

- Autoritatea pentru Digitalizarea României - discuții privind aplicarea Legii nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea.

- Ministerul Cercetării, Inovării și Digitalizării – având în vedere prevederile Legii nr. 214/2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea, au fost puse în discuție aspecte referitoare la elaborarea normelor privind procedura de supraveghere, control și sancționare a prestatorilor de servicii de încredere.

- Ministerul Mediului, Apelor și Pădurilor – discuții privind monitorizarea transporturilor de materiale lemnoase printr-un sistem de supraveghere de tip LPR ce permite recunoaşterea plăcutelor de înmatriculare a vehiculelor.

- Oficiul Național de Prevenire și Combatere a Spălării Banilor – discuții privind implementarea la nivel național a Directivei (UE) 2024/1640 a Parlamentului European și a Consiliului privind mecanismele care trebuie instituite de statele membre pentru prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Directivei (UE) 2019/1937 și de modificare și abrogare a Directivei (UE) 2015/849.

- Secretariatul General al Guvernului – Grup de lucru creat la nivelul Secretariatului General al Guvernului în cadrul căruia au avut loc mai multe întâlniri în format fizic și on-line în vederea elaborării Strategiei Naționale privind Datele Deschise, document realizat pe baza analizei detaliate a contextului social, administrativ, economic și informațional în care se realizează, în prezent, publicarea datelor deținute de entitățile publice, în raport cu standardele și așteptările europene.

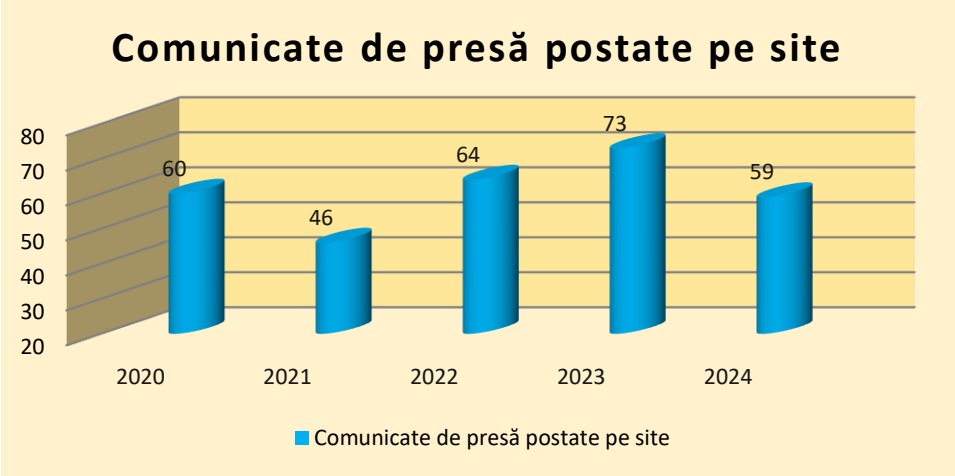
- Secretariatul General al Guvernului –Grup de lucru în cadrul căruia au fost puse în discuție aspecte privind aplicarea la nivel național a Regulamentului (UE) 2023/1804 al

Parlamentului European și al Consiliului privind instalarea infrastructurii pentru combustibili alternativi și de abrogare a Directivei 2014/94/UE.

Totodată, 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, dar și prin intermediul celor **aprox. 4.000 de consultații telefonice,** în cadrul programului zilnic de relații cu publicul, cu privire la modalitatea de punere în practică a prevederilor Regulamentului (UE) 2016/679, fiind 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 2024 o informare promptă şi eficientă cu privire la activitatea desfășurată, atât prin prisma celor **59 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.



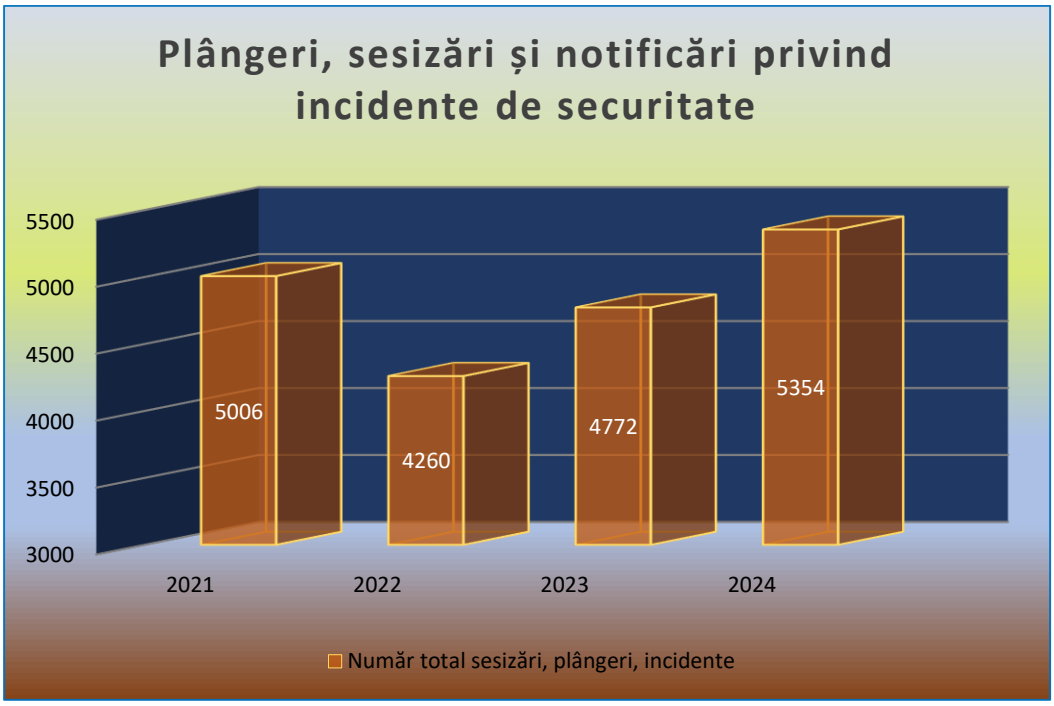
CAPITOLUL III

ACTIVITATEA DE MONITORIZARE ȘI CONTROL

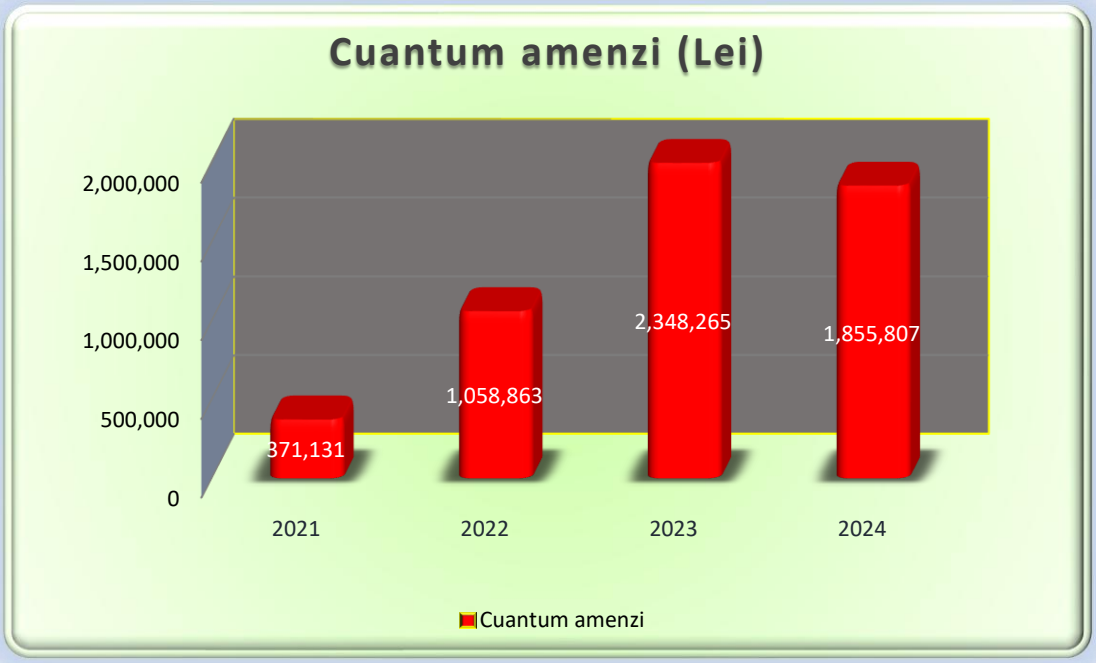
Secțiunea 1: Prezentare generală

În cursul anului 2024, Autoritatea Națională de Supraveghere a primit un număr de **5354** de plângeri, sesizări și notificări privind incidente de securitate.

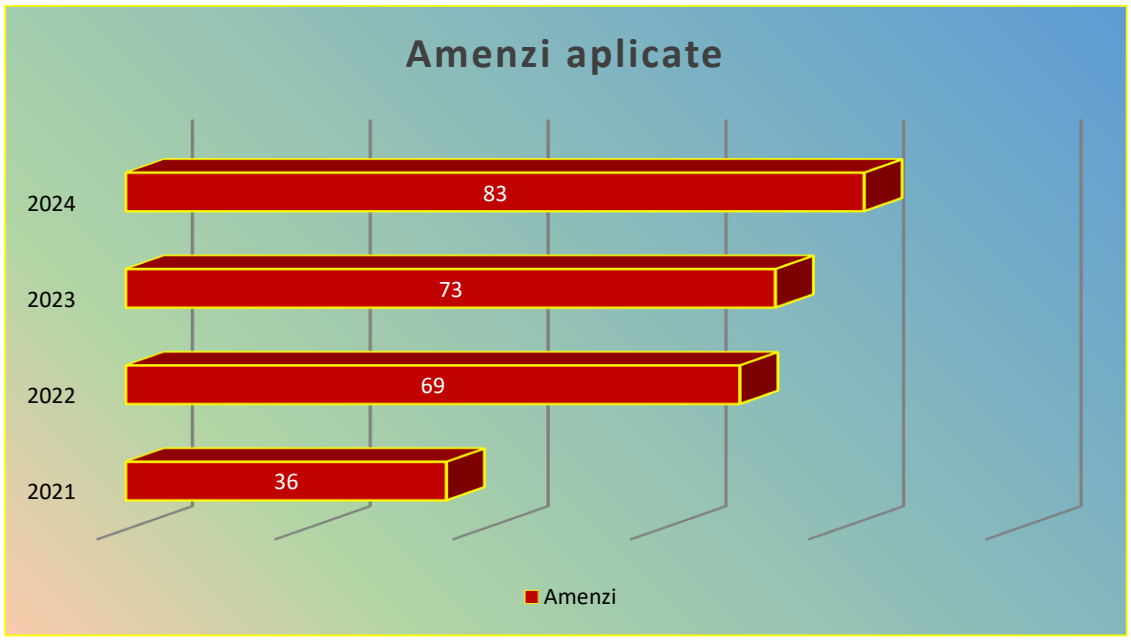
De asemenea, în anul 2024 au fost finalizate **476 investigații**.



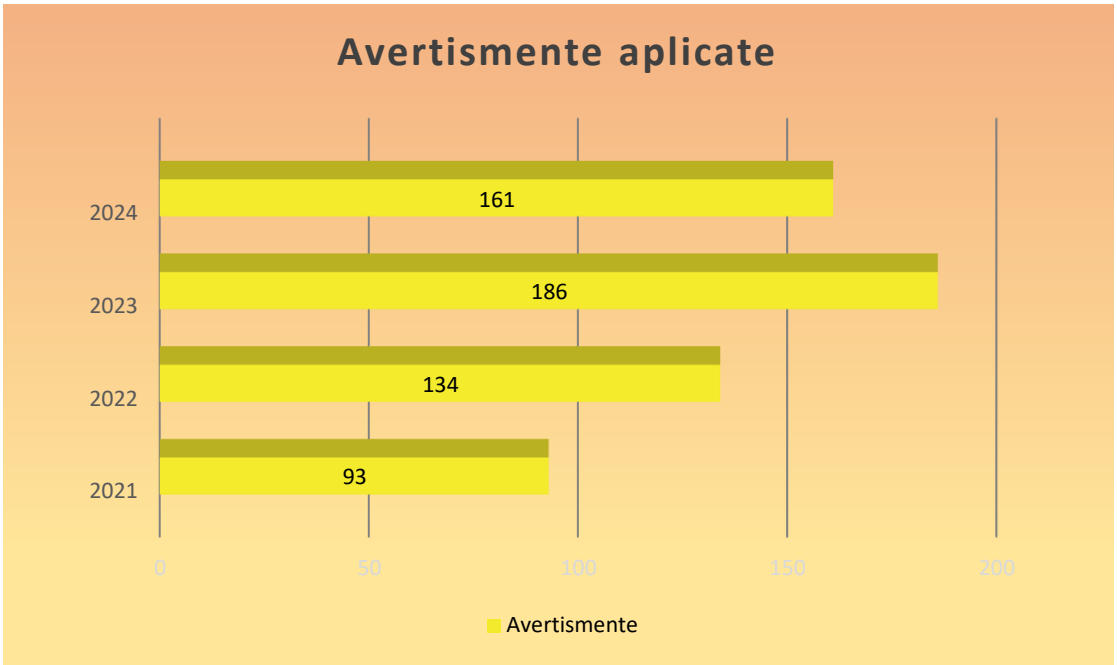
Ca urmare a investigațiilor efectuate, Autoritatea națională de supraveghere a aplicat, în anul 2024, în total **83 de amenzi** în cuantum total **de 1.855.807 lei - echivalentul sumei de 335.100 Euro.**



Dintre acestea**, 80 de amenzi** au fost aplicate în baza Regulamentului (UE) 2016/679 (în cuantum de **1.676.807 lei**), **2 amenzi** au fost aplicate în baza Legii nr. 506/2004 (în cuantum de **20.000 lei)** și **1 amendă** a fost aplicată în baza Legii nr. 190/2018 (în cuantum de **159.000 lei**).



De asemenea, în anul 2024, au mai fost aplicate în total **161 de avertismente**, au fost dispuse **180 de măsuri corective, 4 avertizări** și au fost emise **2 decizii.**



În anul 2024, plângerile înregistrate la Autoritatea națională de supraveghere au vizat, în principal, următoarele aspecte:

- nerespectarea drepturilor persoanelor vizate;
- încălcarea principiilor de prelucrare a datelor;
- dezvăluirea datelor cu caracter personal către terți în spațiul public, în mediul online, inclusiv în cadrul rețelelor de socializare;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video de către persoane fizice și persoane juridice;
- raportarea de date la Biroul de Credit;
- primirea de mesaje comerciale nesolicitate.

Prin intermediul sesizărilor transmise în anul 2024 au fost semnalate, în principal, aspecte referitoare la:

- 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 online ca urmare a configurării deficitare a site-urilor/aplicațiilor informatice utilizate de operatori;
- divulgarea neautorizată a credențialelor de acces în diferite platforme de gestiune a angajaților;
- prelucrarea datelor cu caracter personal prin intermediul sistemelor de supraveghere video, inclusiv prin utilizarea unor mijloace de supraveghere video mobile (body-cam);
- 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.

Referitor la încălcarea securității datelor cu caracter personal, în cursul anului 2024, notificările transmise Autorității naționale de supraveghere au vizat, în principal, următoarele aspecte:

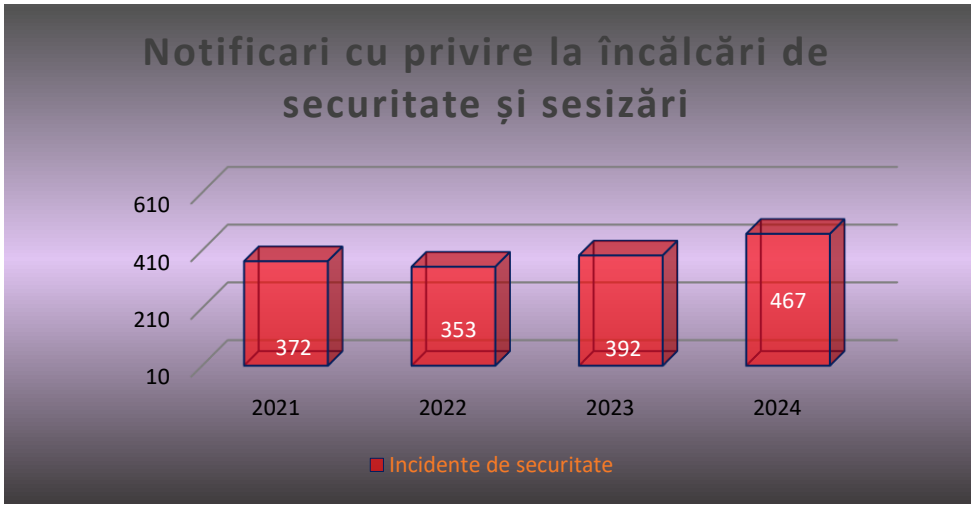
- confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare a dezvăluirilor neautorizate ori ca urmare a unui incident informatic de tip atac ransomware;
- confidențialitatea datelor cu caracter personal în mediul online;
- pierderea confidențialității și accesul neautorizat a datelor cu caracter personal (inclusiv date medicale) în mediul online;
- confidențialitatea datelor cu caracter personal prin nerespectarea principiului privacy by design/privacy by default;
- prelucrarea datelor cu caracter personal ale clienților din sistemul bancar;
- accesul neautorizat la sistemele de supraveghere video cu circuit închis;
- dezvăluirea datelor cu caracter personal în sistemul medical.

Secțiunea a 2-a: Investigații din oficiu

I. Prezentare generală

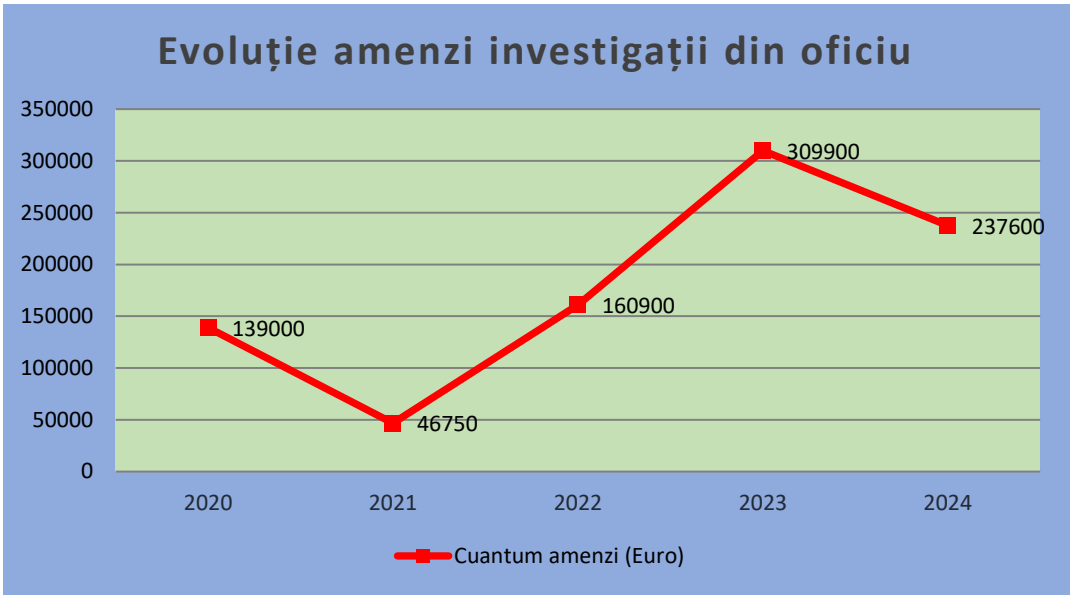
În cursul anului 2024, a continuat activitatea de monitorizare și control a operatorilor din sectorul public și privat, urmărindu-se cu prioritate obiective legate de respectarea prevederilor Regulamentului (UE) 2016/679, ale Legii nr. 190/2018, dar și ale Legii nr. 506/2004.

În anul 2024, Autoritatea națională de supraveghere a primit un număr total de **467 sesizări și notificări** de încălcare a securității datelor cu caracter personal, dintre care **297 sesizări și 170 încălcări de securitate a datelor cu caracter personal.**

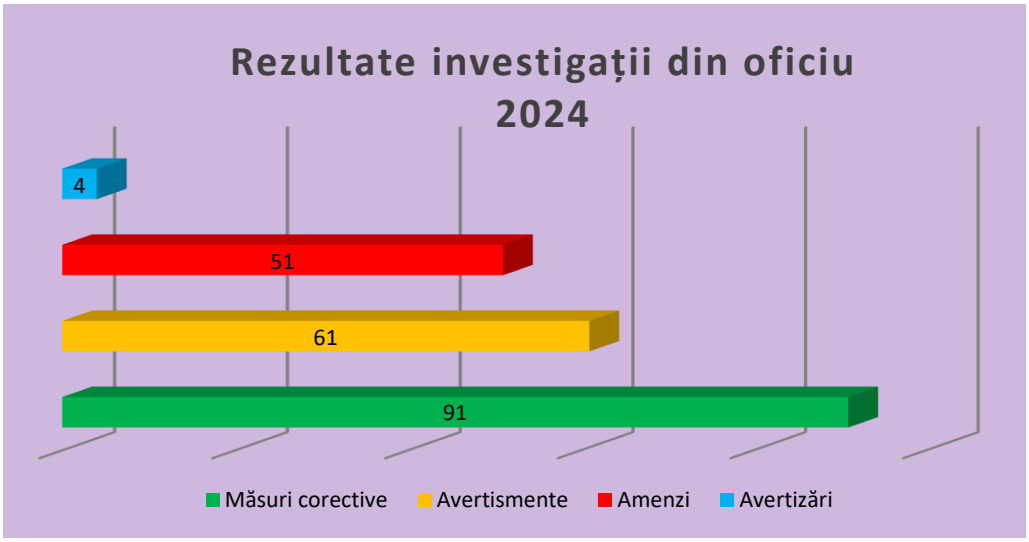


Pe baza sesizărilor și notificărilor de încălcare a securității datelor cu caracter personal au fost demarate **investigații** într-un număr de **342** cazuri.

Ca urmare a investigațiilor din oficiu efectuate au fost aplicate **51 amenzi** în **cuantum total de 237.600 Euro** în baza **Regulamentului (UE) 2016/679,2 amenzi** în baza **Legii nr. 506/2004** în cuantum total de 20.000 lei și **o amendă** în baza **Legii 190/2018** în cuantum total de 159.000 lei.



De asemenea, în investigațiile din oficiu efectuate au fost aplicate **61 avertismente**, **4 avertizări** și au fost dispuse **91 măsuri corective**.



În anul 2024, prin intermediul **sesizărilor** transmise au fost semnalate, în principal, aspecte referitoare la:

- 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 online ca urmare a configurării deficitare a site-urilor/aplicațiilor informatice utilizate de operatori;
- divulgarea neautorizată a credențialelor de acces în diferite platforme de gestiune a angajaților;
- prelucrarea datelor cu caracter personal prin intermediul sistemelor de supraveghere video, inclusiv prin utilizarea unor mijloace de supraveghere video mobile (body-cam);
- 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.

Referitor la încălcarea securității datelor cu caracter personal, în cursul anului 2024, **notificările** transmise Autorității naționale de supraveghere au vizat, în principal, următoarele aspecte:

- confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare a dezvăluirilor neautorizate ori ca urmare a unui incident informatic de tip atac ransomware;
- confidențialitatea datelor cu caracter personal în mediul online;
- pierderea confidențialității și accesul neautorizat la datele cu caracter personal în mediul online;
- confidențialitatea datelor cu caracter personal prin nerespectarea principiului privacy by design/privacy by default;
- prelucrarea datelor cu caracter personal ale clienților din sistemul bancar;
- accesul neautorizat la sistemele de supraveghere video cu circuit închis;
- dezvăluirea datelor cu caracter personal în sistemul medical.

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;
- implementarea tehnică și organizatorică, anterior lansării în producție, a unui plan de testare a tuturor componentelor/aplicațiilor ce se doresc a fi introduse în cadrul activităților care includ prelucrări de date cu caracter personal, prin analizarea tuturor funcționalităților acestora într-un mediu de test, care să simuleze scenariul real din mediul de producție;

- efectuarea unei evaluări de impact asupra datelor cu caracter personal raportat la prevederile Deciziei ANSPDCP nr. 174/2018;
- implementarea tehnică și organizatorică a unor măsuri de diminuare a riscului încălcării confidențialității datelor cu caracter personal prin atac informatic;
- asigurarea conformității prelucrării datelor cu caracter personal, inclusiv prin asigurarea ca transmisiunile de date cu caracter personal să se realizeze exclusiv prin mijloace de comunicații securizate la nivelul tuturor site-urilor operatorului.

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

În anul 2024, Autoritatea națională de supraveghere a efectuat investigații din oficiu privind prelucrarea datelor cu caracter personal de către autorități și instituții publice, instituții de învățământ din domeniul public și privat.

Acestea s-au concentrat pe verificarea respectării dispozițiilor Regulamentului (UE) 2016/679, cu privire la desemnarea responsabilului cu protecția datelor (art. 37 – art. 39), 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) și la utilizarea de sisteme care presupun prelucrarea datelor biometrice pentru control acces (amprente, imagini faciale etc.).

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

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

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

1. FIȘĂ DE CAZ - atac cibernetic

În urma unui articol apărut în presă referitor la faptul că datele personale ale unor cetățeni români ar fi fost scoase la licitație pe internet în urma unui atac cibernetic care a vizat Direcția fiscală și Poliția locală a unui municipiu, instituția noastră a demarat o investigație din oficiu la unitatea administrativ-teritorială respectivă.

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 rezultat în extragerea neautorizată a unui număr foarte mare de documente conținând date cu caracter personal, inclusiv acte de identitate, acte de proprietate, adrese și date de contact.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru contravenția prevăzută de art. 14 alin. (2) lit. a) din Legea nr. 190/2018, prin raportare la dispozițiile art. 83 alin. (4) lit. a) din Regulamentul (UE) 2016/679, pentru încălcarea art. 32 alin. (1) lit. b) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

Sancțiunea a fost însoțită de măsura corectivă de a implementa și actualiza o procedură de notificare a încălcării securității datelor cu caracter personal care să cuprindă inclusiv modul de raportare și tratare a incidentelor de securitate.

2. FIȘĂ DE CAZ – amendă cominatorie aplicată unei autorități publice locale

Autoritatea națională de supraveghere a demarat o investigație la un operator din sectorul public, ca urmare a unor sesizări referitoare la o posibilă încălcare a prevederilor legale cu privire la prelucrarea datelor de către acesta, prin intermediul unei platforme online utilizate pentru colectarea datelor cu caracter personal, achiziționate înainte ca proiectul de hotărâre să fie dezbătut și aprobat în cadrul consiliului local.

Întrucât operatorul nu a comunicat către Autoritatea națională de supraveghere informațiile solicitate în baza competențelor sale de investigare, acesta a fost sancționat cu avertisment. Sancțiunea avertismentului a fost însoțită de un plan de remediere prin

care s-a dispus măsura de a furniza/comunica toate informațiile solicitate de Autoritatea națională de supraveghere.

Ulterior, având în vedere că operatorul nu a transmis informațiile solicitate în termenul dispus de Autoritatea națională de supraveghere, în aplicarea art. 14 alin. (5) lit. e) din Legea nr. 190/2018, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 10.000 lei.

Prin același proces-verbal, s-a aplicat și măsura corectivă constând în obligația operatorului de a furniza/comunica toate informațiile solicitate anterior, necesare pentru soluționarea sesizărilor primite.

Operatorul nu a dat curs nici de această dată solicitării de informații adresate de Autoritatea națională de supraveghere în termenul de 10 zile de la data comunicării celui de-al doilea proces-verbal.

În consecință, operatorul a fost sancționat cu amendă cominatorie în cuantum de 159.000 lei, prin decizie a președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal. Amenda cominatorie a fost calculată pentru 53 de zile întârziere.

Precizăm că, potrivit prevederilor art. 18 alin. (2) din Legea nr. 102/2005 privind înființarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată, Autoritatea națională de supraveghere poate dispune, prin decizie, aplicarea unei amenzi cominatorii de până la 3.000 lei pentru fiecare zi de întârziere, calculată de la data stabilită prin decizie, în cazul nerespectării măsurilor dispuse sau în cazul refuzului tacit sau expres de furnizare a tuturor informațiilor și documentelor solicitate în cadrul procedurii de investigație ori în cazul refuzului de supunere la investigație.

3. FIȘĂ DE CAZ - prelucrarea datelor biometrice din cadrul unei instituții de învățământ

În urma apariției unui articol într-un cotidian național despre o instituție de învățământ public cu privire la o posibilă încălcare a dispozițiilor privind protecția datelor cu caracter personal prin utilizarea a două sisteme de control acces prin recunoaștere facială, Autoritatea națională de supraveghere s-a sesizat din oficiu și a demarat o investigație la sediul unității de învățământ.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat că operațiunile de prelucrare a datelor cu caracter personal prin utilizarea funcției de recunoaștere facială a sistemului de control acces pentru digitalizarea fluxurilor de mobilitate a elevilor ar fi putut să încalce prevederile art. 5 alin. (1) lit. a) și lit. c) din Regulamentul (UE) 2016/679 prin raportare la art. 6 din Regulamentul (UE) 2016/679, astfel încât să fie adusă o atingere dreptului la viață privată și la protecția datelor cu caracter personal a elevilor și personalului propriu din cadrul operatorului.

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.

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

În anul 2024, 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 și sesizările referitoare la activitatea de prelucrare a datelor cu caracter personal au vizat, în principal, divulgarea sau accesul neautorizat la datele cu caracter personal, încălcarea principiilor de prelucrare și încălcarea confidențialității datelor în mediul online.

Ca urmare a investigațiilor efectuate în sectorul privat au fost aplicate operatorilor sancțiuni contravenționale în cuantum total de 1.211.730 lei în baza Regulamentului (UE) 2016/679 și a Legii nr. 506/2004, cât și măsuri corective.

1. FIȘĂ DE CAZ - Compromiterea confidențialității datelor

Un operator ce activează în domeniul serviciilor medicale a notificat o încălcare a confidențialității datelor cu caracter personal a unui număr semnificativ de persoane fizice constând în redirecționarea automată a e-mailurilor adresate operatorului către o ”căsuță de e-mail externă”. Eroarea la transmiterea e-mailurilor a fost semnalată administratorului mesageriei electronice de către utilizatori.

Verificările interne ale operatorului au relevat un atac cibernetic de tip malware, prin care atacatorul a obținut credențialele la căsuța de e-mail; acest fapt a avut drept

consecință redirecționarea automată, configurată, către o altă adresă de e-mail. Astfel, au fost redirecționate multe mesaje pe e-mail, conținând în atașamente rezultate ale analizelor medicale specifice domeniului de activitate al operatorului (informații imagistice, analize de laborator).

Urmare a investigației efectuate, s-a reținut că operatorul nu a implementat un proces de testare/monitorizare periodică a integrității conturilor generice de e-mail cu privire la configurația aplicațiilor prin intermediul cărora funcționează serviciul de e-mail, eroarea la trimiterea e-mailurilor fiind semnalată de utilizatori.

Autoritatea națională de supraveghere a constatat în cadrul investigației că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea sistemelor și serviciilor de prelucrare și un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Potrivit art. 5 alin. (1) lit. f) din Regulamentul (UE) 2016/679, operatorul avea obligația de a prelucra datele cu caracter personal (cel puțin date de identificare precum nume și prenume, adrese de e-mail, date privind starea de sănătate cuprinse în rezultatele analizelor de laborator și investigații imagistice) într-un mod care asigură securitatea adecvată a acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("confidențialitate").

Aceasta a condus la divulgarea și accesarea neautorizată a datelor cu caracter personal prin redirecționarea către o adresă de e-mail a unui terț a numeroase e-mailuri destinate adresei de oficiale de poștă electronică a operatorului.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 24.864 lei (echivalentul în lei al sumei de 5.000 de Euro), pentru încălcarea art. 32 alin. (1) lit. b) și lit. d), coroborat cu art. 32 alin. (2) din Regulamentul (UE) 2016/679, însoțită de măsura corectivă constând în implementarea unui proces de testare, evaluare și monitorizare periodică a integrității conturilor generice de e-mail cu privire la configurația aplicațiilor prin intermediul cărora funcționează serviciul de e-mail.

2. FIȘĂ DE CAZ - Prelucrare nelegală prin încălcarea principiilor de prelucrare a datelor cu caracter personal

Un operator din domeniul bancar a notificat o încălcare a securității datelor cu caracter personal constând în transmiterea din eroare, prin e-mail, către un număr foarte mare de foști clienți, a unei informări având ca scop avertizarea acestora cu privire la fraudele online.

Transmiterea destinată clienților utilizatori de carduri și Internet/Mobile Banking, a fost generată de o eroare operațională umană survenită la momentul generării bazei de date către care urma a fi trimisă informarea, de către un angajat al operatorului, prin includerea în baza de date cu destinatari a adreselor de e-mail ale unor foști clienți ai băncii.

În cadrul investigației s-a constatat că operatorul stochează timp de 5 ani datele persoanelor fizice cărora le-au fost refuzate cererile de împrumut, respectiv 10 ani de la terminarea relației contractuale pentru persoanele fizice vizate care dețin/au deținut produsele băncii;

Autoritatea națională de supraveghere a reținut că respectarea obligației de păstrare/arhivare a documentelor și înregistrărilor, pentru o perioadă de 5 ani după încetarea relației contractuale cu un client și a obligației de monitorizare a tranzacțiilor/operațiunilor efectuate de clienții unei bănci, nu echivalează cu legalitatea prelucrării în continuare a datelor personale ale acestora (adică a altor operațiuni decât stocarea datelor), în cazul persoanelor care nu mai desfășoară o relație de afaceri activă cu banca.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul a încălcat prevederile art. 5 alin. (1) lit. a), b) și f) și alin. (2) din Regulamentul (UE) 2016/679, prin raportare la dispozițiile art. 6 alin. (1) și art. 32 alin. (4) din Regulamentul (UE) 2016/679, prelucrând nelegal datele (adrese de e-mail) foștilor clienți, după data încetării relațiilor contractuale cu aceștia, într-un scop incompatibil cu cel prevăzut de Legea nr. 129/2019 și Regulamentul BNR nr. 2/2019 (ce impunea doar păstrarea/arhivarea datelor cu caracter personal), fără temei legal și într-un mod care nu asigură securitatea adecvată a datelor cu caracter personal.

Operatorul a fost sancționat cu amendă în cuantum de 24.842 lei (echivalentul în lei al sumei de 5.000 Euro), însoțită de măsura corectivă constând în monitorizarea

desfășurării activităților de prelucrare a datelor cu caracter personal ale persoanelor care acționează sub autoritatea operatorului, în conformitate cu procedurile de lucru.

3. FIȘĂ DE CAZ - Prelucrarea nelegală de către un operator a copiilor cărților de identitate ale propriilor angajați

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o societate a transmis pe e-mail copiile cărților de identitate ale propriilor angajați, fără acordul acestora, către o altă societate, pentru formare profesională în vederea calificării profesionale ca agenți de securitate.

În cadrul investigației efectuate, nu s-au putut prezenta dovezi din care să rezulte faptul că procedura utilizată de operator a fost în conformitate cu Regulamentul (UE) 2016/679.

Astfel, Autoritatea națională de supraveghere a constatat faptul că societatea a încălcat prevederile art. 5 alin. (1) lit. a) și alin. (2) raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679, deoarece a utilizat datele cu caracter personal – copia cărții de identitate (nume, prenume, cod numeric personal, serie și nr. carte de identitate, adresă domiciliu, sex, cetățenie, locul nașterii și poză), prin divulgarea prin transmitere a copiilor cărților de identitate ale propriilor angajați, prin intermediul adresei de e-mail, în vederea calificării profesionale ca agenți de securitate, fără să existe o obligaţie legală a operatorului și fără a face dovada îndeplinirii vreunei condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Pentru această faptă, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 49.744 lei, echivalentul a 10.000 Euro pentru încălcarea art. 5 alin. (1) lit. a) și alin. (2) raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Totodată, s-a dispus față de operator măsura corectivă de a prelucra datele cu caracter personal ale persoanelor care sunt desemnate să participe la cursuri de formare profesională, cu respectarea regulilor și principiilor prevăzute de art. 5 și art. 6 din Regulamentul (UE) 2016/679.

Ulterior, operatorul a transmis dovada plății amenzii, cât și informații privind modalitatea de îndeplinire a măsurilor dispuse prin procesul verbal emis de către Autoritatea națională de supraveghere.

4. FIȘĂ DE CAZ - Divulgarea și accesul neautorizat la datele cu caracter personal prelucrate de către o unitate sanitară

O clinică medicală a notificat Autoritatea națională de supraveghere prin completarea formularului privind încălcarea securității datelor cu caracter personal conform Regulamentului (UE) 2016/679, cu privire la accesul neautorizat și la încălcarea confidențialității datelor cu caracter personal ale unui număr semnificativ de persoane fizice.

Operatorul a notificat faptul că un angajat a efectuat un back-up al datelor salvate pe laptop-ul de serviciu (nume și prenume, cod numeric personal, data nașterii, vârsta, sex, număr de telefon de serviciu sau personal, adresă de e-mail de serviciu sau personală, informații cu privire la adresa de corespondență, tipul abonamentelor, informații cu privire la ofertare, număr accesări într-un an, valori plăți într-un an, ultima locație accesată, , numele medicului, voce, opinii exprimate în apeluri telefonice legate de ofertare, ultima specialitate accesată, , calitatea de angajat al societății, profesia, funcția, pontaje, , salarizare, bonusuri primite, zile de concediu de odihnă, locul de desfășurare a activității, calitatea de angajat) pe un hard disk extern personal, acesta fiind păstrat la domiciliu de către angajat. Având intenția să utilizeze hard disk-ul personal pentru media sharing – filme, muzică, pe propriul TV, toate datele cu caracter personal ale unui număr semnificativ de persoane vizate, ale căror date erau prelucrate de către societate, au fost expuse pe internet.

Ca urmare a investigației efectuate, s-a constatat faptul că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de confidențialitate și securitate corespunzător riscului prelucrării și nu a luat măsuri suficiente pentru a asigura că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucrează decât la cererea sa. Aceasta a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal pe internet, prin partajarea acestora cu ajutorul unui dispozitiv mobil de stocare, ale unui număr semnificativ de persoane vizate, deși avea această obligație potrivit art. 5 alin. (1) lit. f din Regulamentul (UE) 2016/679 - principiul ,,integritate și confidențialitate”.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 24.856 RON, echivalentul sumei de 5.000 Euro pentru încălcarea art. 32 alin. (1) lit. b), alin. (2) și alin. (4) din Regulamentul (UE) 2016/679.

De asemenea, s-a dispus măsura corectivă de revizuire și actualizare a măsurilor tehnice și organizatorice implementate inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal, precum și realizarea unei instruiri pentru persoanele autorizate să prelucreze date asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale.

Ulterior, clinica medicală a transmis dovada plății, cât și documente și informații privind modalitatea de îndeplinire a măsurilor dispuse de către instituția noastră.

5. FIȘĂ DE CAZ – Divulgarea și accesul neautorizat la date

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că un site care aparține unei societăți comerciale nu afișează informarea privind drepturile specifice conferite de Regulamentul (UE) 2016/679 și nici informarea privind politica de utilizare cookies.

La data efectuării investigației, s-a constatat faptul că operatorul nu respecta prevederile art. 13 alin. (1) lit. a) din Regulamentul (UE) 2016/679, întrucât nu afișa clar denumirea/identitatea operatorului responsabil de prelucrarea datelor cu caracter personal pe site-ul care îi aparține.

De asemenea, s-a constatat că, prin accesarea website-ului administrat de operator, se instalau module cookies înainte de acordarea consimțământului acestuia și care nu erau necesare din punct de vedere tehnic în funcționarea site-ului.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea prevederilor art. 13 alin. (1) lit. a) din Regulamentul (UE) 2016/679 și cu amendă în cuantum de 10.000 lei pentru încălcarea art. 4 alin. (5) lit. a) din Legea nr. 506/2004.

6. FIȘĂ DE CAZ – Accesul neautorizat la datele cu caracter personal prin intermediul unor atacuri informatice

Un magazin de comerț electronic a notificat Autoritatea națională de supraveghere, prin completarea a două formulare privind încălcarea securității datelor cu caracter personal conform Regulamentului (UE) 2016/679, cu privire la accesul neautorizat și la încălcarea confidențialității datelor cu caracter personal, astfel:

a) Operatorul a fost informat prin e-mail de către un terț cu privire la faptul că unele conturi ale clienților acestuia au fost publicate pe o platformă, fiind afectate date cu caracter personal ale unui număr foarte mare de persoane vizate, respectiv: nume, prenume, e-mail, parola cont, informații disponibile în contul de client, precum adresă de livrare, nr. telefon, istoric comenzi, date referitoare la cardurile cu care se efectuează plata online, comunicări în relația cu operatorul;

b) Operatorul a constatat că a fost victima unui atac informatic de tip „credential stuffing", prin încercări repetate de validare a parolelor asupra unor conturi ale clienților pentru plasarea de comenzi de carduri cadou; s-a precizat că au fost afectate, pentru un număr semnificativ de persoane vizate, următoarele date cu caracter personal: nume, prenume, adresa e-mail, parola acces cont client, date financiare referitoare la carduri bancare înregistrate în aplicație/site.

În cadrul investigației s-a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prezentat de prelucrare, pentru a preveni accesarea în mod ilegal a conturilor clienților operatorului. Aceasta a condus la accesul neautorizat la datele cu caracter personal ale unui număr foarte mare de clienți ai operatorului prin intermediul a două atacuri informatice distincte ce au presupus preluarea controlului asupra unor conturi.

Astfel, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 99.516 lei, echivalentul a 20.000 Euro pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și ale 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 tehnică și organizatorică a următoarelor măsuri de diminuare a riscului încălcării confidențialității datelor cu caracter personal prin atac informatic asupra platformelor de autentificare în conturile de client de pe toate site-urile/aplicațiile de comerț electronic gestionate: notificare logare dispozitiv nou, afișarea dispozitivelor logate în cont, politică de complexitate și istoric a parolelor asupra tuturor conturilor de client cu un interval de expirare a acesteia prestabilit;

- implementarea tehnică și organizatorică a unui sistem de monitorizare a traficului de internet de intrare și de ieșire (inbound/outbound) executat asupra platformelor de

autentificare în conturile de client de pe toate site-urile/aplicațiile de comerț electronic gestionate.

7. FIȘĂ DE CAZ - Divulgarea și accesul neautorizat la datele cu caracter personal ale clienților unei bănci

O instituție financiar-bancară a transmis Autorității Naționale de Supraveghere trei notificări cu privire la producerea unor încălcări a securității datelor cu caracter personal, astfel:

a) operatorul a fost sesizat de către un client care reclama contractarea unui credit în numele său;

b) operatorul a notificat faptul că doi angajați ai săi au furnizat informații confidențiale despre tranzacțiile unui client către un fost angajat al băncii prin utilizarea rețelelor sociale Meta, Messenger și WhatsApp, care la rândul său le-a transmis mai departe unor rude ale clientului;

c) operatorul a fost sesizat de către un client care reclama existența unor produse nesolicitate de către acesta, precum și lipsa unor sume de bani din contul său.

În cadrul investigației efectuate s-a constatat faptul că instituția financiar-bancară nu a luat măsuri pentru a se asigura că orice persoană fizică care acționează sub autoritatea sa și are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, ceea ce a condus la accesul neautorizat și/sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate prin aplicațiile informatice utilizate de operator în activitatea de creditare de către angajatul acestuia.

Astfel, s-au efectuat anumite tranzacții neautorizate de retragere numerar și operațiuni de transfer bancar în numele mai multor persoane vizate, fiind afectate următoarele categorii de date cu caracter personal: numele, prenumele, codul numeric personal, adresa de domiciliu/reședința și de corespondență, numărul de telefon fix/mobil, data nașterii, numele și adresa angajatorului, ip-ul de produs, starea produsului/contului, data acordării, termenul de acordare, sumele acordate, sumele datorate, data scadenței, valuta, frecvența plaților, suma plătită, rata lunară, sumele restante, numărul de rate restante, numărul de zile de întârziere, categoria de întârziere, data închiderii produsului, numărul de interogări, istoric tranzacții, contracte direct debit, depozite, cont economii, fonduri de investiții.

De asemenea, s-a constatat accesul neautorizat și divulgarea neautorizată a datelor unui client (nume, prenume, cod numeric personal, adresa de domiciliu/corespondență, număr de cont, data tranzacțiilor, suma tranzacțiilor, beneficiarii plăților) prin transmiterea acestora către persoane terțe de către doi angajați ai băncii prin utilizarea rețelelor Facebook, Messenger și Whatsapp. În cadrul investigației, s-a reținut și faptul că, începând din anul 2015 până în luna martie a anului 2023, au fost accesate și divulgate neautorizat datele cu caracter personal ale mai multor clienți ai băncii ca urmare a acțiunilor efectuate de un angajat al operatorului în scopul obținerii unor produse financiare în numele persoanelor vizate afectate.

Ca atare, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 99.466 lei, echivalentul a 20.000 Euro, pentru încălcarea prevederilor art. 32 alin. (4) coroborat cu art. 32 alin. (1) lit. b) și d) și alin. (2) din Regulamentul (UE) 2016/679.

De asemenea, s-au dispus operatorului următoarele măsuri corective:

- implementarea tehnică și organizatorică a unui plan care să includă un proces de testare, evaluare și apreciere periodică a tuturor acțiunilor de introducere/actualizare date cu caracter personal pentru persoanele vizate (clienți), inclusiv notificarea și acordul clientului în orice formă asupra oricărei modificări a datelor cu caracter ce pot fi efectuate de către angajații operatorului;

- în vederea asigurării informării regulate privind riscurile prelucrării neautorizate a datelor cu caracter personal de către angajați, se impune diseminarea acestor informații, la un interval de cel mult 6 luni, inclusiv cu necesitatea probării luării la cunoștință de către fiecare dintre angajații care au acces la date cu caracter personal și atribuții în activitatea curentă de prelucrare a datelor clienților.

8. FIȘĂ DE CAZ – Încălcarea confidențialității datelor cu caracter personal de către un furnizor de energie electrică

Un furnizor de energie electrică a notificat Autoritatea națională de supraveghere, prin completarea unui formular privind încălcarea securității datelor cu caracter personal conform Regulamentului (UE) 2016/679, cu privire la divulgarea neautorizată ce a avut loc în cadrul și în momentul lansării unei aplicații informatice a operatorului, ca urmare a unei erori tehnice.

În cadrul investigației, s-a constatat că încălcarea securității datelor cu caracter personal a avut loc în cadrul și în momentul lansării aplicației operatorului, ca urmare a unei erori tehnice și a neefectuării unei testări suficiente a acesteia. Această situație a condus la pierderea integrității și disponibilității datelor cu caracter personal, respectiv la divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal aparținând unui număr semnificativ de persoane vizate.

Autoritatea națională de supraveghere a sancționat furnizorul de energie electrică cu amendă în cuantum de 74.562 Lei (echivalentul sumei de 15.000 Euro) pentru încălcarea prevederilor art. 25 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

Totodată, s-a dispus față de operator măsura corectivă de implementare a unui plan de testare în mediul de test, care să simuleze scenariul real din producție în toate situațiile plauzibile din mediul de producție, anterior lansării în producție a tuturor componentelor/aplicațiilor ce se doresc a fi introduse în cadrul activităților care includ prelucrări de date cu caracter personal.

9. Fișă de caz - Divulgarea neautorizată sau accesul neautorizat la date cu caracter personal în sectorul medical

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, la cabinetul de recoltare (punct de lucru) al unui operator din sectorul medical, sunt expuse public (lipite pe monitorul calculatorului) credențialele de acces la contul de e-mail al cabinetului.

Conform informațiilor furnizate de petent, în cadrul contului de e-mail erau stocate date cu caracter personal, inclusiv date sensibile ale pacienților, acesta devenind vulnerabil și accesibil oricui se afla în proximitatea calculatorului.

În cadrul investigației, s-a constatat că operatorul nu a adoptat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea datelor cu caracter personal ale unor persoane vizate, ceea ce a permis un acces neautorizat la acestea, cel puțin la data reclamării incidentului.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 9.953 Lei (echivalentul sumei de 2.000 Euro), pentru încălcarea dispozițiilor art. 32 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:

- instruirea persoanelor care acționează sub autoritatea operatorului, referitor la obligațiile ce le revin conform prevederilor Regulamentul (UE) 2016/679, inclusiv cu privire la riscurile și consecințele pe care le implică prelucrările de date cu caracter personal;
- adoptarea unei politici actualizate privind parolele care să cuprindă inclusiv reguli cu privire la respectarea confidențialității credențialelor de utilizatori.

C. Investigații tematice din oficiu

În anul 2024, Autoritatea națională de supraveghere a efectuat investigații tematice în baza planului anual de control tematic care au avut ca scop verificarea modului de prelucrare a datelor cu caracter personal la nivelul unităților sanitare, unităților de învățământ și instituțiilor publice. În ceea ce privește unitățile de învățământ și instituțiile publice, menționăm că nu a constatat încălcări ale prevederilor legale privind protecția datelor cu caracter personal.

Dintre investigațiile efectuate, exemplificăm:

- **Centru medical privat**

Autoritatea națională de supraveghere a demarat o investigație din oficiu la un operator privat care activează în domeniul serviciilor medicale, iar ca obiect al controlului s-a urmărit:

- verificarea respectării dispozițiilor Regulamentului (UE) 2016/679 cu privire la desemnarea responsabilului cu protecția datelor (art. 37 – art. 39);
- verificarea respectării prevederilor Regulamentului (UE) 2016/679 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).

Din analizarea informațiilor primite, s-a reținut că operatorul privat care oferea servicii medicale nu a prezentat dovezi din care să rezulte că a elaborat un registru de evidență a cazurilor de încălcare a securității datelor cu caracter personal și că nu exista nici un plan de răspuns la incidentele de securitate.

Autoritatea națională de supraveghere a recomandat operatorului privat care oferea servicii medicale, elaborarea unui registru de evidență a cazurilor de încălcare a securității și detalierea unui plan de răspuns la incidentele de securitate.

Operatorul a dat curs recomandărilor emise de Autoritatea națională de supraveghere și a luat măsuri tehnice și organizatorice împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau a deteriorării accidentale, în temeiul prevederilor Regulamentului (UE) 2016/679.

- **Spital clinic de urgență – operator public**

Autoritatea națională de supraveghere a demarat o investigație tematică solicitând informații inclusiv cu privire la o notificare de încălcare a securității datelor cu caracter personal transmisă de un operator public din domeniul sănătății (spital).

În urma verificărilor efectuate s-a constatat că operatorul a încălcat art. 32 alin. (4) coroborat cu art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679, deoarece nu a luat măsuri tehnice și organizatorice pentru a se asigura că orice persoană fizică care acționează sub autoritatea operatorului și are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern.

De asemenea, s-a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea și integritatea sistemelor și serviciilor de prelucrare pentru a garanta securitatea prelucrării.

Aceasta a condus la accesul neautorizat și/sau divulgarea neautorizată a datelor cu caracter personal transmise (date medicale), stocate sau prelucrate prin intermediul biletului de ieșire din spital al unei persoane vizate, prin transmiterea unui e-mail de către un angajat al operatorului către adresa oficială de e-mail a unui alt spital, fiind încălcate procedurile și politicile existente la nivelul operatorului.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment în temeiul art. 58 alin. (2) lit. b) din Regulamentul (UE) 2016/679, raportat la art. 83 alin. (4) lit. a) din Regulamentul (UE) 2016/679, coroborate cu art. 14 alin. (11) și art. 15 alin. (1) din Legea nr. 102/2005, republicată, precum și în temeiul art. 12 din Legea nr. 190/2018, coroborat cu

art. 7 din OG nr. 2/2001, pentru încălcarea dispozițiilor art. 32 alin. (4) și art. 32 alin. (1) lit. a) și alin. (2) din Regulamentul (UE) 2016/679.

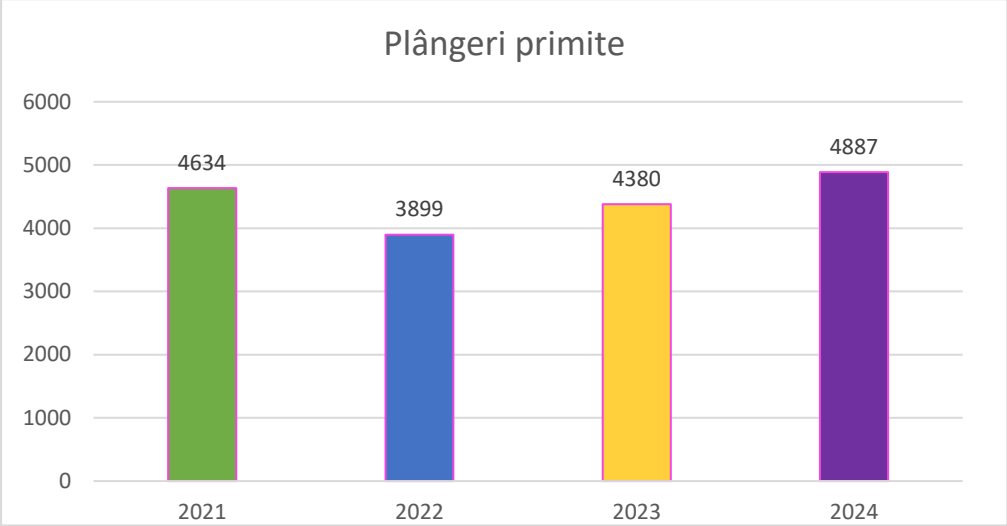
Totodată operatorului i s-a aplicat și măsura de remediere, menționată în planul de remediere, de a instrui angajații cu privire la riscurile pe care le implică prelucrările de date cu caracter personal, pentru evitarea unor incidente similare de divulgare neautorizată a datelor cu caracter personal ale persoanelor fizice vizate.

Secţiunea a 3-a: Activitatea de soluționare a plângerilor

Prezentare generală

În anul 2024, în exercitarea competențelor prevăzute de Regulamentul (UE) 2016/679 și a legislației naționale de implementare a prevederilor acestuia, respectiv Legea nr. 102/2005, republicată, precum și Legea nr. 190/2018, Autoritatea națională de supraveghere a primit un număr total de **4887 plângeri**, care au vizat, în principal, următoarele aspecte:

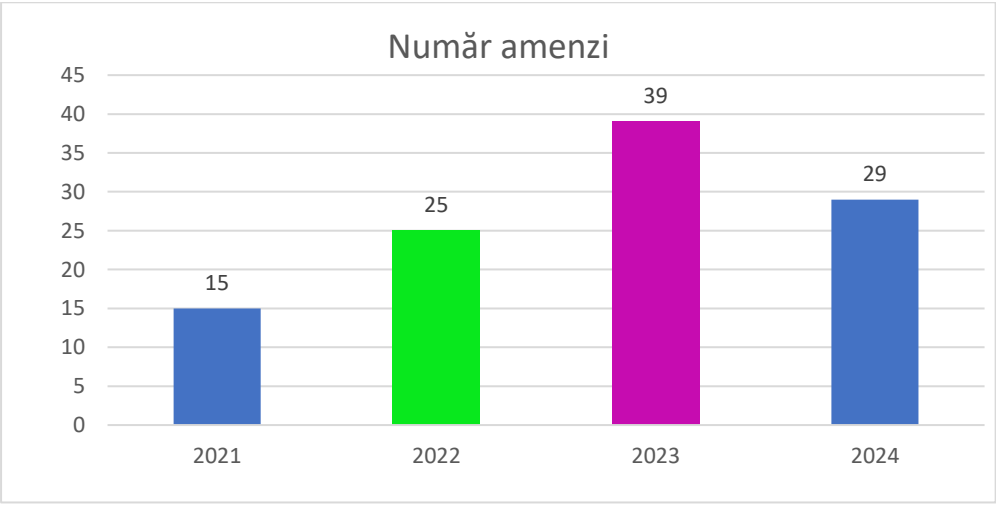
- nerespectarea drepturilor persoanelor vizate;
- încălcarea principiilor de prelucrare a datelor;
- dezvăluirea datelor cu caracter personal către terți în spațiul public, în mediul online, inclusiv în cadrul rețelelor de socializare;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video de către persoane fizice și persoane juridice;
- raportarea de date la Biroul de Credit;
- primirea de mesaje comerciale nesolicitate.

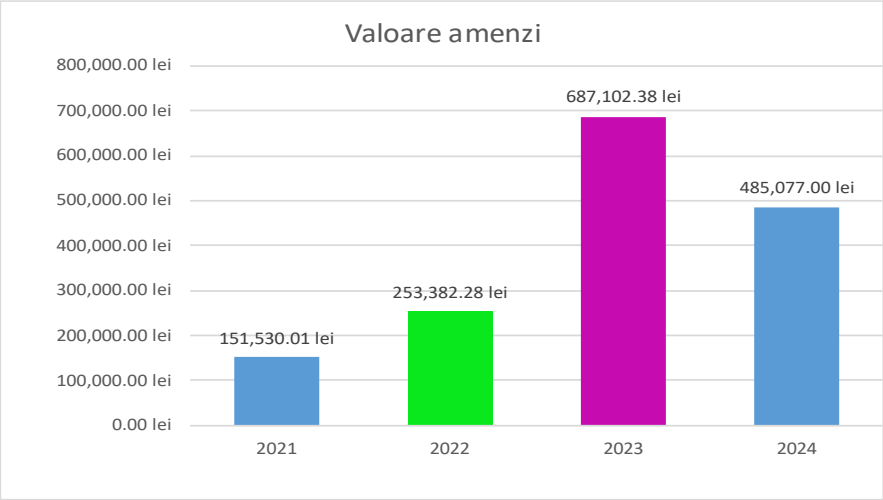


Pentru soluționarea plângerilor considerate admisibile au fost demarate **258 de investigații.**

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

- **29 amenzi în baza Regulamentului (UE) 2016/679,** reprezentând un cuantum total de 485.077 lei (echivalentul sumei de 97.500 Euro);
- **100 de avertismente;**
- **89 măsuri corective,** în baza dispozițiilor art. 58 alin. (2) lit. a), c) și d) din Regulamentul (UE) 2016/679.

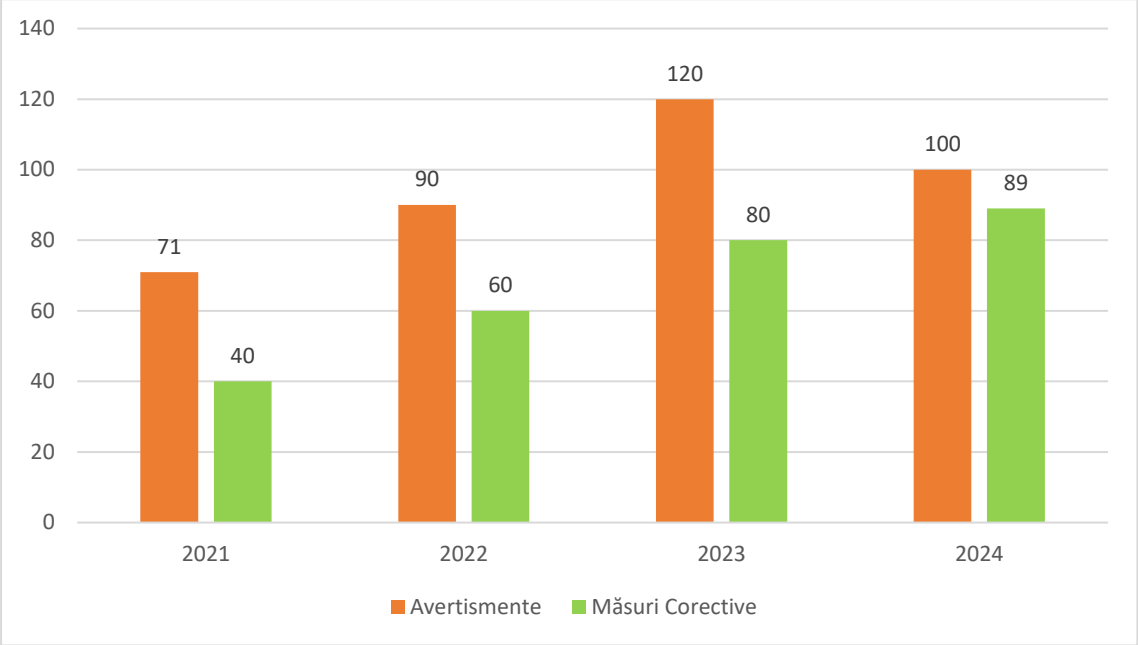




Măsurile corective aplicate de Autoritatea naţională de supraveghere au avut ca obiect în principal următoarele:

- asigurarea conformității operațiunilor de prelucrare cu dispozițiile Regulamentului (UE) 2016/679;
- adoptarea măsurilor tehnice și organizatorice necesare, inclusiv sub aspectul instruirii corespunzătoare a personalului propriu, astfel încât operatorul să fie în măsură să analizeze, să soluționeze în mod corect și să răspundă la toate cererile prin care persoanele vizate își exercită drepturile, în cadrul termenelor și potrivit condițiilor prevăzute de art. 12-23 din Regulamentul (UE) 2016/679;
- transmiterea unui răspuns la cererea persoanei vizate, prin comunicarea copiei înregistrării imaginilor care o privesc, prelucrate prin intermediul sistemului de supraveghere video, în intervalul orar și locația precizate de persoana vizată, cu respectarea art. 15 din Regulamentul (UE) 2016/679, eventual prin luarea măsurilor de obturare (”blurare”) a acelor date care aduc atingere drepturilor și libertăților altora;
- adoptarea de proceduri interne adecvate și eficiente de protecție a datelor cu caracter personal privind modul de soluționare a cererilor depuse de persoanele vizate în temeiul Regulamentului (UE) 2016/679 (art. 12-22), respectarea în toate cazurile a dispozițiilor aplicabile privind analizarea și soluționarea fără întârziere a cererilor persoanelor vizate, astfel încât operatorul să se asigure că dă curs efectiv cererilor prin care se exercită drepturile persoanelor vizate prevăzute de Regulamentul (UE) 2016/679;

- respectarea principiilor de prelucrare, în special cele prevăzute de art. 5 și art. 6 din Regulamentul (UE) 2016/679, inclusiv prin realizarea unei instruiri corespunzătoare a persoanelor care prelucrează date personale sub autoritatea operatorului și transmiterea unor instrucțiuni adecvate către persoanele împuternicite, potrivit art. 28 din Regulamentul (UE) 2016/679;
- revizuirea procedurilor interne și instruirea regulată a personalul propriu, pentru a se evita situațiile de colectare excesivă a unor date personale în exercitarea atribuțiilor de serviciu, prin raportare la fiecare scop specific al prelucrării și prin folosirea unor mijloace tehnice neadecvate (nesecurizate);
- implementarea de măsuri tehnice și organizatorice adecvate, astfel încât să se asigure confidențialitatea datelor personale prelucrate, precum și luarea unor măsuri de pseudonimizare/anonimizare a datelor personale sau a unora dintre acestea, conform art. 32 din Regulamentul (UE) 2016/679;
- implementarea unor măsuri tehnice și organizatorice adecvate și eficiente care să asigure respectarea principiului integrității și confidențialității (art. 5 alin. (1) lit. f) din Regulamentul (UE) 2016/679), astfel încât să se evite situațiile în care pe site-ul operatorului sunt postate documente ce conțin date cu caracter personal;
- adoptarea unor măsuri de obturare a datelor personale disponibile în documentele publice afișate pe pagina de internet, cu respectarea condițiilor prevăzute de legislația aplicabilă;
- asigurarea conformității cu Regulamentul (UE) 2016/679 a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin informarea transparentă, corectă și completă a tuturor persoanelor vizate ale căror date personale sunt prelucrate de operator, în conformitate cu dispozițiile art. 12-14 din Regulamentul (UE) 2016/679;
- limitarea perioadei de stocare a datelor personale prin raportare la scopurile prelucrării datelor, conform obligațiilor prevăzute de Regulamentul (UE) 2016/679 și de Legea nr. 190/2018.



1. Principalele constatări din activitatea de soluționare a plângerilor

A. Nerespectarea drepturilor persoanelor vizate reglementate de Regulamentul general privind protecția datelor

Și în anul 2024, nerespectarea drepturilor persoanelor vizate a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere.

Demersurile întreprinse pentru soluționarea plângerilor au evidențiat o serie de deficiențe în respectarea drepturilor persoanelor vizate conform Regulamentului (UE) 2016/679, atât de către operatori din domeniul privat, cât și de către autorități și instituții publice, ceea ce a condus la aplicarea unor sancțiuni și măsuri corective.

Ca urmare a investigațiilor efectuate s-a constatat că operatorii de date fie nu au furnizat răspunsuri adecvate sau în termen legal persoanelor vizate care au solicitat acces la datele lor personale, fie au refuzat să comunice copii ale datelor personale prelucrate, invocând justificări neconforme cu prevederile Regulamentului (UE) 2016/679. În anumite cazuri, operatorii au indicat persoanelor vizate să consulte politicile de confidențialitate, fără a le furniza informațiile concrete solicitate.

Totodată, s-au constatat întârzieri nejustificate în soluționarea cererilor persoanelor vizate, în unele cazuri operatorii răspunzând cererilor cu depășirea termenului legal prevăzut

de art. 12 alin. (3) și (4) din Regulamentul (UE) 2016/679. Justificările invocate de operatori, precum probleme tehnice, restructurări interne sau erori umane, nu au fost considerate argumente valide pentru încălcarea drepturilor persoanelor vizate.

În ceea ce privește dreptul la ștergerea datelor (art. 17 din Regulamentul (UE) 2016/679), în mai multe cazuri, operatorii nu au respectat cererile de ștergere a datelor, continuând prelucrarea acestora fără un temei legal valid. Astfel, au existat situații în care persoanele vizate au continuat să primească mesaje comerciale după ce și-au exercitat dreptul de opoziție și au primit confirmarea ștergerii datelor.

În urma investigațiilor efectuate pentru soluționarea plângerilor, Autoritatea națională de supraveghere a aplicat sancțiuni contravenționale și a dispus operatorilor să asigure mecanisme eficiente și transparente de gestionare a cererilor privind accesul, ștergerea și rectificarea datelor; instruirea periodică a personalului propriu cu privire la obligațiile privind protecția datelor personale; respectarea termenelor legale pentru soluționarea cererilor persoanelor vizate; adoptarea unor măsuri tehnice și organizatorice pentru a preveni incidentele de securitate și prelucrările neautorizate ale datelor; evitarea utilizării adreselor de e-mail necontrolate pentru gestionarea cererilor și asigurarea unor metode alternative de contact accesibile persoanelor vizate.

1. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea unei plângeri prin care un petent a reclamat că operatorul, organizator de evenimente de divertisment, nu i-a trimis niciun răspuns la cererea prin care își exercitase dreptul de acces la date și respectiv, de ștergere a datelor, cu toate că o reiterase în repetate rânduri.

Ca urmare a investigației demarate în acest caz, s-a constatat că operatorul a răspuns cu întârziere (după șase luni) la cererea persoanei vizate, a confirmat ștergerea datelor petentului, însă a omis să îi comunice informațiile solicitate în baza dreptului său de acces.

Astfel, în cadrul investigației, operatorul a invocat mai multe motive pentru a justifica tergiversarea soluționării corecte a cererilor petentului, respectiv: includerea acestora în folderul de ”spam”, restructurările din cadrul companiei și perioada de recrutare a unui nou responsabil cu protecția datelor personale.

Aceste argumente nu au putut fi reținute, întrucât operatorul nu a dovedit că în perioada de ”restructurare” s-a preocupat de verificarea și gestionarea corespunzătoare a

corespondenței primite pe adresa de e-mail dedicată și făcută publică pe site-ul său pentru a răspunde la cererile primite din partea persoanelor vizate. Astfel, chiar și în absența unui responsabil cu protecția datelor personale, subzista obligația operatorului de a răspunde în cadrul termenelor legale la cererile prin care persoanele vizate își exercitau drepturile prevăzute de Regulamentul (UE) 2016/679.

În plus, în măsura în care o anumită perioadă de timp adresa de e-mail dedicată nu a fost verificată în mod regulat, se poate prezuma faptul că nu doar cererile petentului nu au fost gestionate în cadrul termenelor legale, ci și cele primite din partea altor persoane vizate.

De asemenea, în cazul în care accesul la adresa de e-mail ar fi fost dificilă pentru o perioadă de timp, operatorul avea obligația de a stabili alte date de contact funcționale pe care să le aducă la cunoștința persoanelor vizate, de o manieră transparentă, rapidă și accesibilă, pentru a nu restricționa nejustificat și pentru a facilita exercitarea drepturilor acestora, conform art. 12 alin. (1) și (2) din Regulamentul (UE) 2016/679.

În privința dreptului de acces, operatorul a invocat o eroare de apreciere a obiectului cererii petentului, astfel că, după ștergerea datelor, nu ar mai fi fost posibil să îi comunice informațiile prevăzute de art. 15 din Regulamentul (UE) 2016/679. Pentru informații suplimentare, petentului i-a fost indicată parcurgerea ”Politicii de confidențialitate” de pe site-ul operatorului.

Or, o astfel de gestionare a cererii de acces este contrară dispozițiilor art. 12 și 15 din Regulamentul (UE) 2016/679, întrucât operatorul avea obligația să acorde prioritate cererii de acces, prin punerea la dispoziția petentului a tuturor informațiilor legate de prelucrarea datelor sale (potrivit art. 15 alin. (1) și (2) din Regulamentul (UE) 2016/679) și a copiei datelor personale (conform art. 15 alin. (3) din Regulamentul (UE) 2016/679), abia ulterior putând să ia măsuri de ștergere a datelor din bazele sale de date.

Pe de altă parte, la data formulării răspunsului către petent, operatorul prelucra în continuare date sale personale, corespunzătoare cererilor prin care acesta și-a exercitat drepturile de acces și ștergere. În plus, trimiterea către ”Politica de confidențialitate” de pe site-ul operatorului nu reprezintă o modalitate adecvată de gestionare a unei cereri de acces, având în vedere particularitățile fiecărui caz de prelucrare a datelor personale ale unei persoane vizate, prin raportare la scopul/scopurile prelucrării, datele personale efectiv prelucrate, destinatarii cărora le-au fost dezvăluite datele, perioada de stocare, etc., toate aceste informații necesitând a fi individualizate în funcție de fiecare persoană vizată.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că, prin modul superficial în care au fost abordate cererile petentului, acestuia i-a fost încălcat dreptul de acces la date, așa cum este acesta reglementat de art. 15 din Regulamentul (UE) 2016/679, necomunicându-i în cadrul termenelor legale, prevăzute de art. 12 alin. (3) și (4) din Regulamentul (UE) 2016/679, nici informații specifice legate de prelucrarea datelor sale personale, nici copia datelor sale personale, așa cum figurau acestea în sistemul de evidență al operatorului la data primirii cererilor.

Față de cele constatate, operatorul a fost sancționat contravențional cu:

1. amendă în cuantum de 49.741 lei (echivalentul a 10.000 Euro), pentru încălcarea art. 15 coroborat cu art. 12 alin. (3) și (4) din Regulamentul (UE) 2016/679;

2. amendă în cuantum de 24.870,5 lei (echivalentul a 5.000 Euro), pentru încălcarea art. 17 alin. (1) coroborat cu art. 12 alin. (3) și (4) din Regulamentul (UE) 2016/679.

În același timp, s-au dispus față de operator și următoarele măsuri corective:

- de a transmite un răspuns scris la cererea persoanei vizate în conformitate cu dispozițiile art. 15 din Regulamentul (UE) 2016/679;

- de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin adoptarea măsurilor tehnice și organizatorice necesare, inclusiv sub aspectul instruirii corespunzătoare a personalului desemnat în acest scop, astfel încât operatorul să fie capabil să analizeze, să soluționeze în mod corect și să răspundă la toate cererile prin care persoanele vizate își exercită drepturile, în cadrul termenelor și potrivit condițiilor prevăzute de art. 12-23 din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ

O petentă a sesizat Autoritatea națională de supraveghere cu privire la încălcarea dreptului de acces și a dreptului de ștergere, de către o companie de telefonie mobilă. În fapt, petenta a solicitat operatorului comunicarea anumitor informații cu privire la datele sale cu caracter personal, precum și ștergerea datelor sale transmise către baza de date ce conține informații despre utilizatorii care nu și-au respectat obligațiile de plată (Preventel).

În cursul desfășurării investigației, Autoritatea națională de supraveghere a constatat că operatorul nu a făcut dovada că a transmis un răspuns petentului la cererea sa de exercitare a drepturilor de acces și ștergere în termen de 30 de zile, răspunsul fiindu-i comunicat de operator după efectuarea demersurilor de către instituția noastră.

Față de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 14930 lei (echivalentul a 3.000 Euro), pentru încălcarea prevederilor art. 15 alin. (3) din Regulamentul (UE) 2016/679.

Totodată, instituția noastră a dispus operatorului și măsura corectivă de a adopta proceduri interne privind modul de soluționare a cererilor depuse de persoanele vizate în temeiul Regulamentului (UE) 2016/679 (art. 12-22), respectarea în toate cazurile a dispozițiilor aplicabile privind analizarea și soluționarea fără întârziere a acestor cereri și comunicarea unor răspunsuri către persoanele vizate în cadrul termenelor legale, precum și instruirea regulată a personalului operatorului.

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

3. FIȘĂ DE CAZ

O petentă a transmis Autorității naționale de supraveghere o plângere prin care a reclamat faptul că o companie de telefonie mobilă i-a încălcat dreptul de acces, refuzând să îi comunice înregistrarea unei convorbiri telefonice purtate cu un angajat al său, referitor la comunicarea unei oferte. În fapt, operatorul și-a justificat refuzul motivând că apelurile telefonice efectuate către/de la Serviciul de Relații cu Clienții, sunt utilizate doar în scopul îmbunătățirii serviciilor și produselor oferite clienților, ca mijloc de probă, sau pentru a fi puse la dispoziția autorităților în baza atribuțiilor legale ale acestora.

Potrivit art. 15 din Regulamentul (UE) 2016/679, persoana vizată are dreptul de a obține o serie de informații cu privire la prelucrarea datelor sale personale. Art. 15 alin. (3) din același act normativ, prevede că ”Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării.”

Persoana vizată trebuie să aibă acces la datele cu caracter personal colectate care o privesc, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia.

Comunicarea unei înregistrări audio ce conține date (voce) care privesc persoana vizată, ca urmare a exercitării dreptului de acces de către aceasta, reprezintă o obligație a operatorului.

În ceea ce privește formatul în care ar trebui furnizate datele cu caracter personal, întrucât vocea persoanei vizate reprezintă o dată cu caracter personal, persoanei vizate

trebuie să îi fie furnizată copia înregistrării acesteia. În mod excepțional, accesul persoanei vizate la datele sale (în speță, voce) poate fi acordat de operator prin furnizarea unei transcrieri a conversației, de exemplu, dacă persoana vizată și operatorul sunt de acord asupra acestei modalități de asigurare a accesului la date.

Comunicarea unei înregistrări audio ce conține date (voce) care privesc persoana vizată se efectuează de operator prin luarea unor măsuri de obturare a acelor date (ex. numele și prenumele) care ar putea să aducă atingere drepturilor și libertăților altor persoane fizice (ex. angajat al operatorului), dacă este cazul.

Prin urmare, operatorul este obligat să adopte o serie de măsuri tehnice și organizatorice, pentru a permite deplina exercitare a dreptului de acces al persoanei vizate, cu respectarea în același timp a drepturilor altor persoane fizice.

Urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul nu a respectat dreptul de acces al petentei, prevăzut de art. 15 alin. (3) și art. 12 alin. (3) din Regulamentul (UE) 2016/679, întrucât nu i-a comunicat datele solicitate (convorbirea între aceasta și angajatul operatorului, în cadrul unui apel din call center) cu toate că la data depunerii cererii prin care a solicitat acces la aceste înregistrări, datele sale (voce) erau încă disponibile, neexpirând termenul de stocare a acestor date, stabilit de către operator.

În consecință, s-a dispus sancționarea operatorului cu avertisment, pentru încălcarea art. 15 alin. (3) și art. 12 alin. (3) din Regulamentul (UE) 2016/679.

4. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii unui petent care a continuat să primească pe numărul său de telefon mesaje comerciale de tip SMS, după ce și-a exercitat dreptul de opoziție și ștergere, iar operatorul i-a confirmat ștergerea datelor. Totodată, deși a solicitat de mai multe ori ștergerea datelor sale cu caracter personal, operatorul nu i-a mai transmis niciun răspuns.

Ca urmare a investigației efectuate, s-a constatat faptul că operatorul nu a luat în considerare solicitările de ștergere/opoziție transmise de petent și a continuat să îi transmită mesaje comerciale prin SMS, deși confirmase ștergerea datelor acestuia, încălcându-se astfel prevederile art. 17 și 21 alin. (3) din Regulamentul (UE) 679/2016.

De asemenea, în cursul investigației, s-a constatat că operatorul nu a făcut dovada existenței exprimării consimțământului persoanei vizate pentru transmiterea mesajelor comerciale pe telefon, fiind încălcate astfel prevederile art. 5 alin. (1) lit. a) și b) și ale art. 6 alin. (1) din Regulamentul (UE) 679/2016.

Totodată, a rezultat că operatorul nu i-a comunicat petentului un răspuns nici la alte cereri prin care și-a exercitat drepturile de acces și ștergere, transmise prin e-mail, deși avea această obligație fiind încălcate dispozițiile art. 15 alin. (1) din Regulamentul (UE) 679/2016, raportat la art. 12 din același regulament.

Față de cele constatate, operatorul a fost sancționat contravențional cu:

1. amendă în cuantum de 4.976,3 lei (echivalentul sumei de 1.000 Euro), pentru încălcarea dispozițiilor art. 17 și art. 21 alin. (3) din Regulamentul (UE) 2016/679;

2. amendă în cuantum de 4.976,3 lei (echivalentul sumei de 1.000 Euro), pentru încălcarea dispozițiilor art. 5 alin. (1) lit. a) și b) din Regulamentul (UE) 2016/679;

3. avertisment, pentru încălcarea dispozițiilor art. 15 alin. (3) din Regulamentul (UE) 2016/679 coroborat cu art. 12 din Regulamentul (UE) 2016/679;

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

1. luarea măsurilor adecvate în vederea respectării prevederilor Regulamentului (UE) 2016/679, astfel încât, pe viitor, să se prelucreze datele cu caracter personal ale persoanelor vizate în scop de marketing direct ce vizează utilizarea serviciilor de comunicații electronice (e-mail, telefon), cu obținerea consimțământului expres și prealabil al acestora, inclusiv adoptarea unor proceduri în acest sens.

2. adoptarea unor proceduri interne adecvate și eficiente de protecție a datelor cu caracter personal privind modul de soluționare a cererilor depuse de persoanele vizate în temeiul Regulamentului (UE) 2016/679 (art. 12-22), respectarea în toate cazurile a dispozițiilor aplicabile privind analizarea și soluționarea fără întârziere a acestor cereri, astfel încât operatorul să se asigure că dă curs efectiv cererilor prin care se exercită drepturile persoanelor vizate prevăzute de Regulamentul (UE) 2016/679, precum și instruirea regulată a personalului operatorului.

Ca urmare a demersurilor instituției noastre, operatorul investigat a dat curs măsurilor corective dispuse.

5. FIȘĂ DE CAZ

Un petent a transmis Autorității naționale de supraveghere o plângere prin care a reclamat faptul că o asociație de proprietari i-a încălcat dreptul de acces, deoarece nu i-a comunicat toate datele sale (imagini) prelucrate, într-un anumit interval orar și o locație precizate de acesta, prin intermediul sistemului de supraveghere video instalat în condominiu. Asociația și-a justificat refuzul, motivând că în acea înregistrare mai apăreau și alte persoane, fiind prelucrată și imaginea acestora. Petentul a fost nemulțumit de răspunsul primit.

Potrivit art. 15 alin. (3) și (4) din Regulamentul (UE) 2016/679,

”(3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

(4) Dreptul de a obține o copie menționată la alineatul (3) nu aduce atingere drepturilor și libertăților altora.”

De asemenea, operatorul este obligat să adopte măsuri pentru facilitarea exercitării drepturilor persoanelor vizate (conform art. 12 alin. (2) din Regulamentul (UE) 2016/679), acestea putând include și folosirea unor programe pentru editarea imaginilor/sunetelor, în cazul aplicării într-o situație concretă a art. 15 alin. (3) și (4) din Regulamentul (UE) 2016/679.

Totodată, conform art. 24 și art. 25 din Regulamentul (UE) 2016/679, operatorul este obligat să adopte politici adecvate de protecție a datelor personale, în cadrul măsurilor tehnice și organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul (UE) 2016/679, măsuri ce pot include și pseudonimizarea.

Astfel, comunicarea unei înregistrări video care conține date care privesc persoana vizată, reprezintă o obligație a operatorului și, ca urmare a cererii persoanei vizate, se poate face prin luarea măsurilor de obturare (”blurare”) a acelor date care ar putea să aducă atingere drepturilor și libertăților altora, dacă este cazul. Prin urmare, operatorul este obligat să adopte o serie de măsuri tehnice și organizatorice, pentru a permite deplina exercitare a

dreptului de acces al persoanei vizate, cu respectarea în același timp a drepturilor altor persoane.

Ca urmare a informațiilor transmise în cadrul investigației efectuate, s-a constatat că asociatia de proprietari nu a respectat dreptul de acces al petentului prevăzut de art. 15 alin. (3) din Regulamentul (UE) 2016/679, întrucât nu i-a transmis o copie a imaginilor care îl privesc, prelucrate în intervalul orar și locația precizate de acesta, prin intermediul sistemului de supraveghere video instalat în condominiu.

Față de cele constatate, s-a dispus sancționarea contravențională cu avertisment a asociației de proprietari pentru încălcarea de art. 15 alin. (3) din Regulamentul (UE) 2016/679.

Totodată, s-a dispus operatorului măsura corectivă de a răspunde la cererea petentului, prin comunicarea copiei înregistrării imaginilor care îl privesc, prelucrate prin intermediul sistemului de supraveghere video în condominiu în intervalul orar și locația precizate de acesta, cu respectarea art. 15 alin. (4) din Regulamentul (UE) 2016/679, respectiv prin luarea măsurilor de obturare (”blurare”) a acelor date care aduc atingere drepturilor și libertăților altora.

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

B. 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 2024 au 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 6 din Regulamentul (UE) 2016/679. Totodată, date cu caracter personal, precum: nume, prenume, cod numeric personal, adresă și număr de telefon, au fost expuse în mod necorespunzător în contexte precum 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.

1. FIȘĂ DE CAZ

Un petent a reclamat la Autoritatea națională de supraveghere faptul că un angajat din cadrul unei autorități publice, i-a dezvăluit ilegal datele cu caracter personal în contextul depunerii unei sesizări privind un transport neconform de material lemnos. În fapt, sesizarea transmisă de către petent către autoritatea publică, care conținea date cu caracter personal ale acestuia (nume, prenume, număr de telefon, adresa poștală de domiciliu, adresa email), a fost redirecționată de către angajații operatorului către persoana reclamată, care l-a contactat, ulterior, pe petent.

În urma investigației efectuate s-a constatat că operatorul a încălcat prevederile art. 5 alin. (1) lit. a), f) și alin. (2), coroborate cu art. 6 din Regulamentul (UE) 2016/679, deoarece datele petentului au fost dezvăluite către persoanele reclamate de acesta, în contextul depunerii unei sesizări privind un transport neconform de material lemnos.

Totodată, s-a constatat că, operatorul a încălcat prevederile art. 32 alin. (1), alin. (2) și alin. (4) și art. 29 din Regulamentul (UE) 2016/679, întrucât nu a prezentat dovezi că a implementat, până la data sesizării petentului, suficiente măsuri de securitate, documente ce conțin date cu caracter personal fiind lăsate nesupravegheate la sediile persoanelor/entităților controlate de către operator, fapt ce a condus la accesul neautorizat la datele cu caracter personal ale petentului.

Față de cele constatate s-a dispus sancționarea operatorului, conform prevederilor Legii nr. 190/2018, care reglementează constatarea contravențiilor și aplicarea sancțiunilor autorităților și organismelor publice, cu:

1. avertisment, pentru încălcarea prevederilor art. 5 alin. (1) lit. a), f) și alin. (2), coroborate cu art. 6 din Regulamentul (UE) 679/2016.

2. avertisment, pentru încălcarea prevederilor art. 32 alin. (1), (2) și alin. (4) și art. 29 din Regulamentul (UE) 679/2016.

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

1. revizuirea procedurilor interne și instruirea regulată a personalului propriu în privința necesității de a analiza fiecare situație în parte, în scopul prelucrării datelor personale cu respectarea principiilor și a condițiilor de prelucrare a datelor personale prevăzute de art. 5 și 6 din Regulamentul (UE) 2016/679 și evitarea situațiilor de dezvăluire ilegală sau neautorizată a acestora;

2. stabilirea de măsuri tehnice și organizatorice adecvate, necesare asigurării securității datelor cu caracter personal prelucrate de către operator, astfel încât să se asigure confidențialitatea datelor personale prelucrate, precum și luarea unor măsuri de pseudonimizare/anonimizare a datelor personale sau a unora dintre acestea, conform art. 32 din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ

Printr-o plângere înregistrată la Autoritatea națională de supraveghere, un petent a reclamat un inspectorat județean de poliție referitor la dezvăluirea ilegală a datelor sale cu caracter personal. În fapt, inspectoratul județean de poliție a transmis, în copie, petiția petentului către avocatul care reprezenta persoanele fizice reclamate prin petiție, dezvăluind inclusiv numele, prenumele, codul numeric personal și adresa petentului.

Ca urmare a investigației efectuate, s-a constatat că inspectoratul județean de poliție a încălcat prevederile art. 5 alin. (1) lit. a) și alin. (2) din Regulamentul (UE) 2016/679, raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679, deoarece a divulgat, prin transmitere, datele cu caracter personal ale petentului, către avocatul care reprezenta persoanele fizice reclamate, fără a exista o obligație legală a operatorului sau consimțământul persoanei vizate și fără îndeplinirea vreunei alte condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679, precum și fără respectarea principiului potrivit căruia operatorul avea obligația de a prelucra datele în mod legal, echitabil și transparent față de persoana vizată conform art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679.

În consecință, s-a dispus sancționarea operatorului cu avertisment, conform prevederilor Legii nr. 190/2018 care reglementează constatarea contravențiilor și aplicarea sancțiunilor autorităților și organismelor publice.

Prin planul de remediere s-a dispus măsura de a revizui procedurile interne și de a instrui personalul astfel încât 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 Regulamentul (UE) 2016/679.

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

3. FIȘĂ DE CAZ

Printr-o petiție transmisă Autorității naționale de supraveghere, o persoană fizică a reclamat că, în scopul completării ulterioare a unor documente în vederea încheierii unui proces verbal de contravenție, un polițist din cadrul unui inspectorat județean de poliție i-a fotografiat cu telefonul personal, actul de identitate și permisul auto, fără acordul său. În fapt, petentul nu a fost mulțumit de răspunsul primit din partea inspectoratului județean de poliție la reclamația sa, prin care era informat că operatorul a dispus măsuri în conformitate cu prevederile Legii nr. 360/2002 privind statutul polițistului, în contextul sesizării privind fotografierea cărții de identitate.

În cursul investigației, s-a constatat că inspectoratul județean de poliție nu a prezentat dovezi din care să rezulte că a adoptat suficiente măsuri tehnice și organizatorice adecvate în vederea asigurării confidențialității datelor prelucrate în legătură cu procedura de efectuare a controalelor pe teren și întocmirea actelor de constatare, prin care să fie evitată/interzisă folosirea dispozitivelor personale ale angajaților săi și efectuarea unor operațiuni de fotografiere a datelor/documentelor personale, în legătură cu exercitarea atribuțiilor de serviciu.

Ca urmare a investigației efectuate, s-a constatat că inspectoratul județean a încălcat prevederile art. 22, art. 26 alin. (2) și art. 35 din Legea nr. 363/2018.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a dispus sancționarea contravențională cu avertisment a operatorului, conform prevederilor Legii nr. 190/2018 care reglementează constatarea contravențiilor și aplicarea sancțiunilor autorităților și organismelor publice.

Prin planul de remediere s-a dispus măsura de a revizui procedurile interne și de a instrui regulat personalul propriu, pentru a se evita situațiile de colectare excesivă a unor

date personale în exercitarea atribuțiilor de serviciu, prin raportare la fiecare scop specific al prelucrării și prin folosirea unor mijloace tehnice neadecvate (nesecurizate).

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

4. FIȘĂ DE CAZ

În anul 2024, Autoritatea națională de supraveghere a finalizat o investigație demarată pentru soluționarea plângerii depuse de către o petentă care a reclamat faptul că asociația de proprietari a dezvăluit, pe grupul de WhatsApp al membrilor săi, o notificare prin care aceasta solicita o serie de informații și documente legate de funcționarea asociației și care conținea datele sale cu caracter personal.

În cadrul investigației declanșate, s-a constatat că operatorul a dezvăluit în mod nelegal și excesiv datele petentei (numele, prenumele și adresa de domiciliu), prin postarea pe grupul de WhatsApp al membrilor asociației, contrar prevederilor art. 5 alin. (1) lit. a), c), alin. (2) și ale art. 6 din Regulamentul (UE) 2016/679.

De asemenea, s-a constatat că asociația de proprietari nu a prezentat dovezi cu privire la comunicarea unui răspuns la cererea petentei prin care aceasta și-a exercitat drepturile de acces, ștergere și opoziție, încălcându-se astfel prevederile art. 12 alin. (3) și (4) din actul normativ mai sus menționat.

Totodată, s-a constatat că operatorul nu a prezentat dovezi cu privire la punerea în aplicare a măsurilor corective dispuse prin procesul-verbal de constatare/sancționare încheiat anterior de instituția noastră, încălcând astfel o dispoziție a Autorității naționale de supraveghere, ceea ce constituie contravenția prevăzută de art. 83 alin. (5) lit. e) din Regulamentul (UE) 2016/679.

Față de cele constatate, operatorul a fost sancționat contravențional cu:

1. amendă în cuantum de 994,48 lei (200 Euro) pentru încălcarea art. 5 alin. (1) lit. a), c), alin. (2) și ale art. 6 din Regulamentul (UE) 2016/679;
2. amendă în cuantum de 497,24 lei (100 Euro) pentru încălcarea art. 12 alin. (3) și (4) din Regulamentul (UE) 2016/679;

3. amendă în cuantum de 994,48 lei (200 Euro) pentru încălcarea art. 58 alin. (2) din Regulamentul (UE) 2016/679 prin raportare la dispozițiile enumerate la art. 83 alin. (5) lit. e) și alin. (6) din Regulamentul (UE) 2016/679.

Totodată, asociației de proprietari i s-au aplicat și următoarele măsuri corective:

1. de a transmite un răspuns scris la cererea petentei, pentru a-i comunica informațiile solicitate în baza dreptului de acces și respectiv, măsurile adoptate în urma exercitării drepturilor de ștergere și opoziție;

2. de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, astfel încât datele cu caracter personal ale persoanelor vizate, inclusiv ale membrilor asociației, să fie prelucrate cu stricta respectare a principiilor și regulilor de prelucrare prevăzute în principal de art. 5 și 6 din Regulamentul (UE) 2016/679, sens în care va realiza inclusiv o instruire corespunzătoare a persoanelor care prelucrează date personale sub autoritatea sa și va transmite instrucțiuni adecvate către persoanele împuternicite, potrivit art. 28 din Regulamentul (UE) 2016/679;

3. de a răspunde în scris la cererea petentei, pentru a-i comunica măsurile adoptate în urma exercitării drepturilor de ștergere și opoziție;

4. de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin adoptarea măsurilor organizatorice necesare, inclusiv sub aspectul instruirii corespunzătoare a personalului desemnat în acest scop, astfel încât operatorul să răspundă la cererile prin care persoanele vizate își exercită drepturile, în cadrul termenelor și potrivit condițiilor prevăzute de art. 12-23 din Regulamentul (UE) 2016/679.

5. FIȘĂ DE CAZ

O petentă a reclamat la Autoritatea națională de supraveghere dezvăluirea ilegală a datelor sale cu caracter personal (adresa de e-mail) de către un operator de telefonie mobilă, către mai mulți destinatari. În fapt, petenta a reclamat dezvăluirea mai multor adrese de e-mail (inclusiv adresa sa personală) în cadrul transmiterii unor comunicări privind schimbarea managerului de cont alocat unor clienți persoane juridice din portofoliul operatorului, mesajele fiind trimise prin poșta electronică în două luni diferite, către mai mulți reprezentanți ai clienților și către mai multe persoane fizice.

În cadrul investigației s-a constatat că nu a adoptat suficiente măsuri tehnice și organizatorice pentru a asigura confidențialitatea datelor personale prelucrate, întrucât nu s-

au luat măsuri de ascundere a adreselor de e-mail ale destinatarilor, spre exemplu prin selectarea opțiunii „BCC" ("blind carbon copy"), ceea ce a condus la o divulgare neautorizată a adreselor de e-mail către ceilalți destinatari, cu încălcarea obligațiilor impuse de art. 32 din Regulamentul (UE) 2016/679.

Față de cele constatate, operatorul a fost sancționat cu amendă în cuantum de 24.870,5 lei (5.000 Euro) pentru încălcarea art. 32 din Regulamentul (UE) 2016/679.

Totodată, a fost dispusă măsura corectivă de reevaluare a măsurilor de securitate implementate, astfel încât să se asigure un nivel de securitate adecvat riscului prelucrării, în special sub aspectul instruirii persoanelor care prelucrează date sub autoritatea sa (angajați sau colaboratori), și al verificării regulate a respectării instrucțiunilor transmise acestora.

6. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii formulate de către un petent, care a reclamat dezvăluirea datelor sale cu caracter personal (imaginea, vocea, numărul de înmatriculare al autovehiculului) de către un politist local aflat în exercitarea atribuțiilor de serviciu.

Urmare a investigației efectuate în acest caz, a reieșit că un polițistul local, care se afla în exercitarea atribuțiilor de serviciu privind constatarea încălcării legislației rutiere, a înregistrat cu telefonul mobil personal și, ulterior, a distribuit înregistrarea video din timpul urmăririi autovehiculului, pe un grup de whatsapp constituit la nivelul direcției de poliție locală. Totodată, această înregistrare a fost postată în cadrul unui articol din presa online.

Astfel, Autoritatea națională de supraveghere a constatat că operatorul, politie locala, a încălcat prevederile art. 32 alin. (1), (2), (4) din Regulamentul (UE) 2016/679, deoarece nu a adoptat măsuri de securitate (tehnice și organizatorice) pentru a se asigura că numai persoanele autorizate au acces la datele personale prelucrate (pentru care au autorizare), fapt care a condus la colectarea datelor personale (în special, imaginea, vocea și numărul de înmatriculare a autovehiculului) ale petentului în circumstanțele descrise, date care apoi au fost diseminate de polițistul local către membrii grupului de whatsapp de la nivelul direcției de poliție locală și, ulterior, trasmiterea și postarea înregistrării în cadrul unui articol în presă.

Față de cele constatate, operatorul a fost sancționat cu avertisment pentru încălcarea art. 32 din Regulamentul (UE) 2016/679.

Prin planul de remediere s-a dispus asigurarea conformității cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin implementarea unor măsuri tehnice și organizatorice adecvate, inclusiv sub aspectul instruirii frecvente a persoanelor care prelucrează date sub autoritatea operatorului, astfel încât prelucrarea datelor persoanelor vizate să fie efectuată cu respectarea reglementărilor privind protecția datelor personale.

C. Prelucrarea datelor cu caracter personal ale angajaților

Și în anul 2024, prelucrarea datelor cu caracter personal ale angajaților a făcut obiectul analizei și verificărilor Autorității naționale de supraveghere. Principalele aspecte reclamate de petenți au vizat dezvăluirea datelor cu caracter personal de către angajator, prelucrarea datelor biometrice ale angajaților, prelucrarea datelor angajaților prin intermediul unor sisteme de monitorizare GPS, prelucrarea imaginilor prin intermediul camerelor de supraveghere video instalate la locul de muncă și prelucrarea datelor angajaților prin intermediul noilor tehnologii.

Astfel, tehnologiile moderne permit angajatorilor să monitorizeze angajații prin intermediul a numeroase dispozitive, inclusiv calculatoare de birou și laptop-uri. În astfel de situații, angajatorul are obligația de a demonstra respectarea cel puțin a uneia dintre condițiile de legalitate prevăzute la art. 6 din Regulamentul (UE) 2016/679, în ceea ce privește prelucrarea datelor angajaților și de a furniza acestora o informare clară și completă.

1. FIȘĂ DE CAZ

Un petent, angajat al unei autorități publice (minister), a reclamat faptul că angajatorul a dezvăluit către conducătorii unor structuri interne din minister codurile numerice personale ale angajaților, cu ocazia anunțării programării pentru efectuarea controlului de medicina muncii, trimisă prin e-mail. Astfel, la respectivul mesaj a fost anexat un tabel excel ce cuprindea, pe lângă numele, funcția, departamentul, data și ora programării, inclusiv codul numeric personal al angajaților.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul a dezvăluit excesiv și fără temei legal codurile numerice personale ale

angajaților, cu încălcarea principiilor și a condițiilor de legalitate a prelucrării prevăzute de art. 5 și 6 din Regulamentul (UE) 2016/679.

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

Prin planul de remediere, Autoritatea națională de supraveghere a dispus operatorului să adopte măsuri prin care să se atragă atenția destinatarilor email-ului să nu utilizeze datele personale, în special, codurile numerice personale la care au avut acces, în scopuri incompatibile cu cele pentru care le-a fost transmisă informarea. Totodată, s-a dispus revizuirea procedurilor existente și asigurarea instruirii regulate a persoanelor care prelucrează date personale sub autoritatea operatorului, cu privire la obligația de respectare a principiilor și a regulilor de prelucrare a datelor cu caracter personal în exercitarea atribuțiilor de serviciu, inclusiv în activitatea desfășurată pentru managementul resurselor umane.

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

2. FIȘĂ DE CAZ

Un petent a reclamat utilizarea, fără informarea sa, a unui sistem de monitorizare prin GPS pe un autoturism de serviciu folosit în perioada în care a fost angajat la o societate.

În cadrul investigației demarate, s-a constatat că operatorul a prelucrat datele petentului, colectate prin intermediul sistemului de monitorizare GPS instalat pe mașina de serviciu, pe o perioadă de 6 luni și a continuat să le prelucreze și ulterior datei la care acesta nu mai era angajat al societății, fără să prezinte dovezi din care să rezulte că anterior a folosit alte metode mai puțin intruzive pentru atingerea scopului prelucrării, legat în principal de întocmirea foilor de parcurs și a pontajului lunar. Totodată, operatorul nu a dovedit că a stabilit cu claritate un temei legal al prelucrării datelor colectate prin intermediul sistemului de monitorizare GPS instalat pe mașina de serviciu a petentului, prin raportare la scopurile în care urmau să fie utilizate aceste date, încălcând astfel art. 5 alin. (1) lit. a), c) și (2) și art. 6 din Regulamentul (UE) 2016/679.

Totodată, s-a constatat că operatorul a prelucrat datele petentului fără să prezinte dovezi cu privire la informarea transparentă și completă a persoanei vizate în legătură cu

prelucrarea datelor sale, în conformitate cu art. 12-14 din Regulamentul (UE) 2016/679 și a stocat aceste date fără să prezinte dovezi din care să rezulte că depășirea termenului de 30 de zile, prevăzut de art. 5 din Legea nr. 190/2018, se bazează pe motive justificate, încălcând astfel art. 5 alin. (1) lit. e) și (2) din Regulamentul (UE) 2016/679.

Față de cele constatate, operatorul a fost sancționat contravențional cu:

1. amendă în cuantum de 9.947,6 lei, echivalentul a 2.000 Euro, pentru încălcarea art. 5 alin. (1) lit. a), c) și (2) și art. 6 din Regulamentul (UE) 2016/679;

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

3. avertisment pentru încălcarea art. 5 alin. (1) lit. e) și (2) din Regulamentul (UE) 2016/679.

Ca atare, s-au dispus față de operator și următoarele măsuri corective:

1. de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de colectare și prelucrare ulterioară a datelor personale, în sensul reevaluării necesității atingerii scopurilor propuse prin folosirea datelor provenite din utilizarea sistemului de monitorizare prin GPS instalat pe mașinile de serviciu ale angajaților operatorului, prin raportare la obligațiile prevăzute de Regulamentul (UE) 2016/679 și de Legea nr. 190/2018;

2. de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin informarea transparentă, corectă și completă a tuturor persoanelor vizate ale căror date personale sunt prelucrate de operator, în conformitate cu dispozițiile art. 12-14 din Regulamentul (UE) 2016/679;

3. de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin limitarea perioadei de stocare a datelor prin raportare la scopurile prelucrării datelor, conform obligațiilor prevăzute de Regulamentul (UE) 2016/679 și de Legea nr. 190/2018.

În urma sancționării sale, operatorul ne-a adus la cunoștință că a încetat să mai utilizeze sistemul de monitorizare prin GPS instalat pe autoturismele de serviciu.

3. FIȘĂ DE CAZ

Printr-o petiție transmisă Autorității naționale de supraveghere, un petent a reclamat faptul că o autoritate publică distribuie pe pagina de internet înscrisuri interne care conțin nume, prenume și semnătură, în mod nelegal, nejustificat și cu încălcarea drepturilor persoanelor vizate. În fapt, autoritatea publică a publicat pe pagina sa de internet un fișier

(arhivă „.zip") unde se regăseau procese verbale de recepție, servicii contractate de instituție, precum și un fișier care conținea datele personale ale unor angajați (alții decât cei care au strict atribuții pe linie de achiziții publice), inclusiv datele cu caracter personal ale petentului (nume, prenume și semnătură), publicate fără consimțământul său și fără nicio justificare sau temei legal.

Ca urmare a investigației efectuate în acest caz, s-a constatat că operatorul nu a prezentat dovezi din care să rezulte că a adoptat măsuri tehnice și organizatorice adecvate în vederea asigurării confidențialității datelor cu caracter personal, astfel încât, la data înregistrării plângerii la autoritatea de supraveghere, pe site-ul instituției erau postate înscrisuri interne (inclusiv note) care conțineau nume, prenume și semnătură ale propriilor angajați, cu încălcarea obligațiilor prevăzute de art. 32 din Regulamentul (UE) 2016/679.

Față de cele constatate, s-a dispus aplicarea unui avertisment pentru încălcarea art. 32 din Regulamentul (UE) 2016/679.

De asemenea, prin planul de remediere, s-a pus în vedere operatorului să adopte măsuri constând în:

- implementarea unor măsuri tehnice și organizatorice adecvate și eficiente care să urmărească inclusiv asigurarea confidențialității datelor personale prelucrate, astfel încât să se evite situațiile în care să fie postate pe site-ul instituției documente ce conțin date cu caracter personal, instruirea regulată a persoanelor care prelucrează date sub autoritatea operatorului; în acest sens, procedura/procedurile astfel adoptate, dovezile instruirii persoanelor care prelucrează date sub autoritatea operatorului etc. vor fi transmise, în copie certificată, către Autoritatea națională de supraveghere;

- adoptarea unor măsuri de obturare a datelor personale disponibile în documentele publice afișate pe pagina de internet, cu respectarea condițiilor prevăzute de legislația în vigoare.

4. FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că angajatorul său de la acel moment (o societate de recuperare a creanțelor) utilizează sisteme de monitorizare prin mijloace de comunicații electronice a angajaților aflați în telemuncă, prin intermediul unei aplicații instalate pe laptop-urile acestora, cu încălcarea prevederilor în materia protecției datelor cu caracter personal. În fapt, petentul a sesizat că aplicația utilizată

avea, în principal, următoarele funcționalități: monitorizarea activității pe Internet a angajaților, prezența la locul de muncă, generarea rapoartelor de productivitate, monitorizarea aplicațiilor rulate.

Urmare a demersurilor întreprinse pentru soluționarea plângerii, Autoritatea națională de supraveghere a constatat că, în scopul verificării activității angajaților cu funcții de conducere, aflați în telemuncă, referitor la respectarea reglementărilor interne, diseminarea neautorizată a informațiilor, respectarea programului de lucru și a productivității și oportunitățile de îmbunătățire a eficienței angajaților, operatorul a decis să implementeze o aplicație de monitorizare pe laptop-urile acestora.

La data efectuării investigației, operatorul nu utiliza aplicația de monitorizare a angajaților aflați în telemuncă, aceasta fiind rulată anterior doar într-o perioadă de testare în care a fost implementat un acces limitat la datele colectate prin intermediul aplicației.

În ceea ce privește datele și categoriile de date care urmau să fie colectate prin intermediul aplicației, operatorul a declarat că acestea vizau: nume, prenume, timpul de lucru, activitățile de prelucrare realizate prin intermediul aplicației generează indicatori ce au în vedere să verifice activitatea angajaților vizați, pe baza timpului petrecut pe internet; rapoarte care includ numele aplicațiilor folosite și timpul petrecut de utilizatori în fiecare aplicație, titlurile documentelor sau paginilor web accesate, precum și istoricul de căutare chiar dacă rezultatul găsit în urma căutării nu a fost accesat; numele documentului listat imprimanta folosită și numărul de pagini;cod numeric personal, serie și nr.carte de identitate, adresă, e-mail atunci când sunt conținute în titlul unui document/pagini.

Față de cele de mai sus, Autoritatea națională de supraveghere a constatat că operatorul nu a dovedit în timpul investigației că modalitățile mai puțin intruzive pentru atingerea scopului urmărit de operator, utilizate înainte de implementarea aplicației, au fost ineficiente și nici că a realizat consultarea prealabilă a angajaților, înainte de implementarea unei astfel de aplicații, în conformitate cu prevederile art. 5 din Legea nr. 190/2018.

Astfel, Autoritatea națională de supraveghere a apreciat că interesul legitim ca și temei legal de prelucrare invocat de operator, nu poate fi considerat justificat, raportat la toate operațiunile de prelucrare asupra tuturor datelor sau categoriilor de date care puteau fi prelucrate prin intermediul aplicației de monitorizare.

În consecință, s-a dispus aplicarea unei avertizări cu privire la posibilitatea ca setul de operațiuni de prelucrare a datelor cu caracter personal prevăzute de operator, prin

intermediul aplicației de monitorizare a activității salariaților cu funcții de conducere aflați în telemuncă, să încalce prevederile art. 6 alin. (1) din Regulamentul (UE) 2016/679, ale art. 5 din Legea nr. 190/2018, precum și principiile de prelucrare a datelor cu caracter personal statuate de Regulamentul (UE) 2016/679, astfel încât ar putea fi adusă o atingere dreptului la viață privată și la protecția datelor personale ale angajaților vizați.

CAPITOLUL IV

ACTIVITĂŢI ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE

Activitatea la nivel internațional a Autorităţii naționale de supraveghere a fost reprezentantă în anul 2024 de participarea, atât în format fizic, cât și în format videoconferință, la o serie de grupuri de lucru la nivel european, conferințe, seminare și alte reuniuni ale organismelor Uniunii Europene sau ale Consiliului Europei în domeniul protecției datelor cu caracter personal, precum şi prin implicarea în activitatea desfășurată în cadrul acestora precum Comitetul European pentru Protecția Datelor, respectiv subgrupurile de lucru.

Comitetul european pentru protecția datelor

În anul 2024, Comitetul european pentru protecția datelor a adoptat **15** avize pe marginea proiectelor de decizii ale autorităților de supraveghere referitoare la regulile corporatiste obligatorii pentru operatori/persoane împuternicite de operatori, **1** aviz pe marginea proiectului de cerințe de acreditare a unui organism de monitorizare a unui cod de conduită, în conformitate cu art. 41 din Regulamentul (UE) 2016/679, **1** aviz pe marginea proiectului de cerințe cu privire la aprobarea cerințelor de acreditare a unui organism de certificare în conformitate cu art. 43 alin. (3) din Regulamentul (UE) 2016/679, **5** 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 nr. 1/2023 referitoare la articolul 37 din Directiva privind protecția datelor în materie de aplicare a legii – Aceste orientări oferă îndrumări cu privire la aplicarea art. 37 din Directiva privind protecția datelor în materie de aplicare a legii (Directiva (EU) 2016/680), în special în ceea ce privește garanțiile adecvate legale standard care urmează a fi aplicate de către autoritățile competente în conformitate cu art. 37 alin. (1) literele a) și b) și, în consecință, în legătură cu factorii relevanți pentru a evalua dacă astfel de garanții există. Prin urmare, aceste orientări includ o indicație cu privire la așteptările Comitetului cu privire

la statele membre, în calitate de părți la negocieri, atunci când intenționează să încheie sau să modifice un instrument obligatoriu din punct de vedere juridic între statul(ele) membru(e) în cauză și o țară terță sau o organizație internațională în conformitate cu art. 37 alin. (1) litera e) din Directiva privind protecția datelor în materie de aplicare a legii;

- Orientările nr. 2/2023 privind domeniul tehnic de aplicare al articolului 5 alineatul (3) din Directiva privind viața privată și comunicațiile electronice – Comitetul abordează, în cadrul acestor orientări, aplicabilitatea art. 5 alin. (3) din Directiva privind viața privată și comunicațiile electronice în cazul unor soluții tehnice diferite. Prezentele orientări explică în mod detaliat Avizul nr. 9/2014 al Grupului de lucru „Articolul 29" referitor la aplicarea Directivei privind viața privată și comunicațiile electronice în ceea ce privește amprentarea dispozitivelor (device fingerprinting) și au scopul de a asigura o înțelegere clară a operațiunilor tehnice care intră sub incidența art. 5 alin. (3) din Directiva privind viața privată și comunicațiile electronice. Orientările identifică trei elemente-cheie pentru aplicabilitatea art. 5 alin. (3) din Directiva privind viața privată și comunicațiile electronice: „informații", „echipamentul terminal al unui abonat sau utilizator" și „dobândirea accesului", „stocarea de informații" și „informații stocate", oferind o analiză detaliată a fiecărui element;
- Avizul nr. 4/2024 privind noțiunea de sediu principal al unui operator în Uniune în temeiul articolului 4 alineatul (16) litera (a) din Regulamentul (UE) 2016/679 – Comitetul stabilește în acest aviz că „locul în care se află administrația centrală" a unui operator în Uniune poate fi considerat ca fiind un sediu principal în temeiul art. 4 alin. (16) litera (a) din Regulamentul (UE) 2016/679 numai dacă acesta ia decizii privind scopurile și mijloacele de prelucrare a datelor cu caracter personal și are competența de a dispune punerea în aplicare a acestor decizii. În plus, Comitetul consideră că mecanismul ghișeului unic se poate aplica numai dacă există dovezi că unul dintre sediile operatorului în Uniune ia decizii privind scopurile și mijloacele pentru operațiunile de prelucrare relevante și are competența de a dispune punerea în aplicare a acestor decizii. Prin urmare, atunci când deciziile privind scopurile și mijloacele și competența de a dispune punerea în aplicare a acestor decizii sunt exercitate în afara Uniunii, nu ar trebui să existe un sediu principal în temeiul art. 4 alin. (16) litera (a) din Regulamentul (EU) 2016/679, iar mecanismul ghișeului unic nu ar trebui să se aplice. Totodată, Comitetul subliniază faptul că autoritățile de supraveghere își păstrează capacitatea de a contesta afirmația operatorului pe baza unei examinări obiective a faptelor relevante, solicitând informații suplimentare atunci când este necesar;

- Avizul nr. 8/2024 privind consimțământul valabil în contextul modelelor de consimțământ sau de plată puse în aplicare de platformele online mari – Domeniul de aplicare al acestui aviz se limitează la punerea în aplicare de către platformele online mari a modelelor de „consimțământ sau plată” în care utilizatorilor li se solicită să își dea consimțământul pentru prelucrare în scopul publicității comportamentale. Comitetul subliniază necesitatea ca toate cerințele Regulamentului (UE) 2016/679 să fie respectate, în special cele privind consimțământul valabil, evaluându-se în același timp particularitățile fiecărui caz. Comitetul reamintește prin acest aviz că obținerea consimțământului nu îl scutește pe operator de respectarea tuturor principiilor enunțate la art. 5 din Regulamentul (UE) 2016/679 și nici de respectarea celorlalte obligații prevăzute în Regulamentul (UE) 2016/679. Este esențial să se respecte principiile necesității și proporționalității, limitării scopului, reducerii la minimum a datelor, precum și cel al echității;
- Avizul nr. 11/2024 privind utilizarea recunoașterii faciale pentru eficientizarea fluxului de pasageri în aeroporturi [compatibilitatea cu articolul 5 alineatul (1) literele (e) și (f) și cu articolele 25 și 32 din Regulamentul (UE) 2016/679] – Comitetul subliniază faptul că utilizarea datelor biometrice și, în special, a tehnologiei de recunoaștere facială implică riscuri sporite pentru drepturile și libertățile persoanelor vizate. Aceasta implică o prelucrare de date biometrice care beneficiază de o protecție specială în temeiul art. 9 din Regulamentul (UE) 2016/679.Înainte de a utiliza astfel de tehnologii, chiar dacă acestea ar fi considerate deosebit de eficace, operatorii ar trebui să evalueze impactul asupra drepturilor și libertăților fundamentale ale persoanelor vizate și să analizeze dacă scopul legitim al prelucrării poate fi atins prin mijloace mai puțin intruzive. Domeniul de aplicare al acestui aviz este limitat la compatibilitatea prelucrării cu art. 5 alin. (1) literele (e) și (f) și cu art. 25 și 32 din Regulamentul (UE) 2016/679 în scopul specific de a eficientiza fluxul de pasageri în aeroporturi la patru puncte de control specifice, și anume la punctele de control de securitate, de predare a bagajelor, de îmbarcare și de acces la salonul pentru pasageri;
- Avizul nr. 22/2024 privind anumite obligații care decurg din încrederea acordată persoanei (persoanelor) împuternicite de operator și subcontractantului (subcontractanților) – Comitetul precizează că operatorii ar trebui să dețină informațiile privind identitatea (de ex. numele, adresa, persoana de contact) tuturor persoanelor împuternicite, ale sub-împuterniciților etc. disponibile în orice moment, astfel încât să își poată îndeplini cel mai bine obligațiile în temeiul art. 28 din Regulamentul (UE) 2016/679, indiferent de riscul asociat

activității de prelucrare. În acest scop, persoana împuternicită ar trebui să ofere în mod proactiv operatorului toate aceste informații și ar trebui să le păstreze mereu actualizate. Comitetul menționează în aviz că, în timp ce persoana împuternicită inițială ar trebui să se asigure că propune sub-împuterniciții care oferă suficiente garanții, decizia finală cu privire la contractarea unui anumit sub-împuternicit și responsabilitatea aferentă, inclusiv în ceea ce privește verificarea garanțiilor oferite, aparține operatorului;

- Avizul 28/2024 privind anumite aspecte legate de protecția datelor privind prelucrarea datelor personale în contextul modelelor IA – În aviz se precizează că afirmațiile privind anonimatul unui model IA ar trebui să fie evaluat de autoritățile de supraveghere competente de la caz la caz, deoarece Comitetul consideră că modelele de IA instruite cu date personale nu pot fi considerate, în toate cazurile, anonime. Pentru ca un model IA să fie considerat anonim, atât (1) probabilitatea extragerii directe (inclusiv probabilistice) a datelor cu caracter personal cu privire la persoanele ale căror date cu caracter personal au fost utilizate pentru elaborarea modelului, cât și (2) probabilitatea ca obținerea, intenționat sau nu, a unor astfel de date personale din interogări, ar trebui să fie nesemnificativă, luând în considerare „toate mijloacele care pot fi utilizate în mod rezonabil" de către operator sau de către o altă persoană. Avizul subliniază rolul așteptărilor rezonabile ale persoanelor vizate în realizarea unui test de echilibru. Acest lucru poate fi important având în vedere complexitatea tehnologiilor utilizate în modelele IA și a faptului că, pentru persoanele vizate, poate fi dificil să înțeleagă varietatea posibilelor utilizări și diferitele activități de prelucrare implicate. În acest sens, atât informațiile furnizate persoanelor vizate, cât și contextul prelucrării poate fi printre elementele care trebuie luate în considerare pentru a evalua dacă persoanele vizate se pot aștepta în mod rezonabil ca datele lor personale să fie prelucrate.

În același timp, Comitetul european pentru protecția datelor a adoptat următoarele orientări disponibile spre consultare publică și trimitere de propuneri:

- Orientările nr. 1/2024 privind prelucrarea datelor cu caracter personal în temeiul art. 6 alin. (1) litera (f) din Regulamentul (UE) 2016/679 – Aceste orientări analizează criteriile stabilite la art. 6 alin. (1) litera f) din Regulamentul (UE) 2016/679 pe care operatorii trebuie să le respecte atunci când se angajează să prelucreze date cu caracter personal care sunt necesare în scopul intereselor legitime urmărite de operator sau de o parte terță. Art. 6 alin. (1) litera (f) din Regulamentul (UE) 2016/679 este unul dintre cele șase temeiuri juridice pentru prelucrarea legală a datelor cu caracter personal prevăzute de Regulamentul (UE)

2016/679. Art. 6 alin. (1) litera (f) nu ar trebui să fie tratat nici ca o „ultimă soluție" pentru situații rare sau neașteptate în care se consideră că alte temeiuri juridice nu se aplică și nici nu ar trebui ales automat sau utilizarea sa să fie extinsă în mod nejustificat pe baza percepției conform căreia art. 6 alin. (1) litera (f) este mai puțin constrângător decât alte temeiuri juridice;

- Orientările nr. 2/2024 privind art. 48 din Regulamentul (UE) 2016/679 – Scopul acestor orientări este de a clarifica rațiunea și obiectivul acestei prevederi, inclusiv al interacțiunii sale cu celelalte prevederi ale capitolului V din Regulamentul (UE) 2016/679 și de a oferi recomandări practice pentru operatorii și persoanele împuternicite din UE care pot primi solicitări de la autoritățile din țări terțe de a dezvălui sau transfera date cu caracter personal.

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 corporatiste 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 2024, Autoritatea națională de supraveghere a emis **o** decizie de aprobare a regulilor corporatiste obligatorii pentru persoana împuternicită de operator în calitate de autoritate principală. Totodată, a primit și a analizat cereri de aprobare a BCRs transmise de **40** companii multinaționale. În același timp, Autoritatea națională de supraveghere a asistat alte autorități de supraveghere, acționând în calitate de co-revizor la cererile de aprobare a BCRs transmise de **4** companii în această perioadă și ca membru în echipa de redactare a **2** propuneri de opinie a Comitetului european pentru protecția datelor referitoare la adoptarea regulilor 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 autoritatea de supraveghere în situația în care nu primește un răspuns/nu este mulțumit de răspunsul primit de la operator,
- păstrarea unei evidențe actualizată 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, ce informații 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 2024, Comitetul european pentru protecția datelor a emis 15 avize în temeiul art. 64 din Regulamentul (UE) 2016/679 pe marginea proiectelor 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 Regulamentului (UE) 2016/679. Solicitările venite din partea autorităților de supraveghere din Austria, Belgia, Bulgaria, Cehia, Estonia, Finlanda, Italia, Polonia, Slovenia, Spania și au vizat aspecte referitoare la bugetul Autorității naționale de supraveghere pentru cheltuieli judiciare, investigații demarate privind localizarea persoanelor vizate folosind adresa IP, prelucrarea datelor biometrice pentru realizarea pontajului, condițiile de exercitare a dreptului de acces, autorizarea instituțiilor/organismelor de tipul biroului de credit de către Autoritatea națională de supraveghere, stabilirea reprezentantului pe teritoriul UE, legislația națională de implementare a art. 77-79 din Regulamentul (UE) 2016/679, legislația națională de transpunere a unor directive, accesul la formularele de notificare a încălcărilor de securitate depuse la Autoritatea națională de supraveghere.

Contribuții din perspectiva protecției datelor cu caracter personal

În cursul anului 2024, Autoritatea națională de supraveghere a formulat observații și propuneri pe marginea documentelor transmise de alte autorități/instituții:

- misiuni de aderare și reuniuni cu reprezentanți ai Organizației pentru Cooperare și Dezvoltare Economică (OCDE) – În vederea aderării României la Organizația pentru Cooperare şi Dezvoltare Economică (OCDE), Autoritatea națională de supraveghere a participat la misiunile și reuniunile organizate de OCDE. Pentru atingerea obiectivelor

propuse, au fost derulate o serie de activități de colectare de informaţii de către autoritățile și instituțiile publice și societatea civilă, care au fost incluse în raportul OCDE;

- procesul de autoevaluare a implementării instrumentelor juridice ale OCDE – în cadrul procesului de aderare a României la Organizația pentru Cooperare și Dezvoltare Economică (OCDE), ca urmare a inițierii procesului de autoevaluare a implementării instrumentelor juridice ale OCDE, Autoritatea națională de supraveghere a transmis o serie de propuneri și observații pe marginea fișelor de autoevaluare cu incidență în domeniul protecției datelor cu caracter personal, acestea cuprinzând informații privind legislația (informații care argumentează felul în care legislația este aliniată cu instrumentul), politici (informații privind felul în care politicile guvernamentale corespund instrumentului), practici (informații privind felul în care practicile corespund instrumentului);
- Rezoluția Mișcării Umanitare Internaționale a Crucii Roșii și a Semilunii Roșii – Autoritatea națională de supraveghere a subliniat faptul că o prelucrare de date cu caracter personal trebuie să se realizeze cu respectarea principiilor de protecție a datelor cu caracter personal stabilite la art. 5 din Regulamentul (UE) 2016/679. Printre acestea, se numără cele privind prelucrarea datelor în mod legal, echitabil şi transparent față de persoana vizată (*legalitate, echitate și transparență*), prelucrarea datelor adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (*reducerea la minimum a datelor*), colectarea datelor în scopuri determinate, explicite şi legitime şi prelucrarea ulterioară într-un mod compatibil cu aceste scopuri (*limitări legate de scop*), precum și prelucrarea într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare (*integritate și confidențialitate*). În ceea ce privește *principiul integrității și confidențialității*, a fost evidențiată necesitatea implementării de măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal, prin raportare la riscurile la adresa drepturilor și libertăților persoanelor fizice ale căror date cu caracter personal sunt prelucrate, cu atât mai mult cu cât prelucrarea respectivă poate viza categorii speciale de date cu caracter personal (date privind starea de sănătate). Aceleași dispoziții legale prevăd faptul că operatorul (în cazul de față toți operatorii care prelucrează datele cu caracter personal în scopuri umanitare) este responsabil de respectarea principiilor legate de prelucrarea datelor cu caracter personal şi poate demonstra această respectare (principiul

responsabilității). În același timp, a fost adusă în atenție necesitatea asigurării drepturilor de care beneficiază persoanele vizate în temeiul Regulamentului (EU) 2016/679 (spre exemplu dreptul la informare, dreptul de acces, dreptul la ștergere), precum și a modalităților de exercitare a acestora;

- revizuirea șabloanelor cu informații care urmează a fi puse la dispoziția cetățenilor terți pe site-ul web ETIAS;
- proiectul de Acord de cooperare în domeniul securității între Guvernul Republicii Turcia și Guvernul României – Autoritatea națională de supraveghere a considerat necesară includerea unei mențiuni referitoare la principiul limitării legate de stocare, a recomandat reformularea unei prevederi prin raportare la art. 9 alin. (1) din proiect. De asemenea, a fost înaintată propunerea de includere a sintagmei „as soon as possible", similar cu alin. (3). În același timp, Autoritatea națională de supraveghere a subliniat ca fiind necesară înlocuirea trimiterii la art. 14 cu art. 17 din proiectul de acord, precum și clarificarea sintagmei „ensure of personal data". Totodată, s-a considerat necesară includerea unei prevederi prin care să se precizeze în mod clar faptul ca Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal este autoritatea competenta să monitorizeze legalitatea prelucrării datelor cu caracter personal efectuate potrivit acestui acord;
- pachetul de securitate (noile reguli privind datele API) – Comisia Europeană a publicat un pachet de securitate cu două propuneri de regulament privind informațiile în avans despre pasageri (Advanced Passenger Information (API)): o propunere privind colectarea și transferul de informații în avans despre pasageri (API) pentru facilitarea controalelor la frontierele externe și o propunere privind colectarea și transferul de informații în avans despre pasageri (API) pentru prevenirea, detectarea, investigarea și urmărirea penală a infracțiunilor de terorism și a altor infracțiuni grave, pe marginea cărora Autoritatea națională de supraveghere a transmis o serie de precizări;
- propunerea de Regulament de stabilire a unor norme procedurale suplimentare referitoare la asigurarea respectării Regulamentului (UE) 2016/679 – Comisia Europeană a lansat propunerea Regulament care urmărește raționalizarea cooperării dintre autoritățile naționale de supraveghere a protecției datelor în ceea ce privește asigurarea respectării Regulamentului (UE) 2016/679 în cazurile transfrontaliere. Față de textul propunerii de Regulament, Autoritatea națională de supraveghere a transmis o serie de observații dintre care evidențiem: adoptarea acestei propuneri de Regulament va atrage inaplicabilitatea sau

necesitatea modificării Legii nr. 102/2005, republicată, precum și a procedurilor de soluționare a plângerilor și de efectuare a investigațiilor; formularul de plângere propus de Comisia Europeană este mult mai sumar decât cel propus de Comitetul european pentru protecția datelor, acesta mai mult enumerând cu titlu generic documentele ce trebuie depuse de petent, în loc să includă efectiv informațiile necesare pentru identificarea exactă a petentului, a reprezentantului, a operatorului; în cazul în care se va lăsa la aprecierea petentului, de exemplu, ce informații va indica, legate de operator, acestea vor fi furnizate în mod diferit și incomplet. În același timp, Autoritatea națională de supraveghere a subliniat faptul că propunerea de regulament generează sarcini birocratice excesive suplimentare pentru autoritățile de supraveghere (în special pentru cele cu resurse umane limitate cum este Autoritatea națională de supraveghere) și, prin urmare, aceste prevederi necesită o reevaluare pe fond și formă, astfel încât noul Regulament preconizat să constituie un instrument eficient și clar de lucru;

- scrisoarea Raportorului Special al ONU pentru Apărătorii de Mediu – În ceea ce privește prelucrarea datelor în scop jurnalistic, Autoritatea națională de supraveghere a subliniat că art. 85 din Regulamentul (UE) 2016/679 stabilește faptul că ”Prin intermediul dreptului intern, statele membre asigură un echilibru între dreptul la protecția datelor cu caracter personal în temeiul prezentului regulament şi dreptul la libertatea de exprimare şi de informare, inclusiv prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare.” Totodată, potrivit art. 7 din Legea nr. 190/2018, în vederea asigurării unui echilibru între dreptul la protecția datelor cu caracter personal, libertatea de exprimare și dreptul la informație, prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare poate fi efectuată, dacă aceasta privește date cu caracter personal care au fost făcute publice în mod manifest de către persoana vizată sau care sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată, prin derogare de la următoarele capitole din Regulamentul general privind protecția datelor: a) capitolul II - Principii; b) capitolul III - Drepturile persoanei vizate; c) capitolul IV - Operatorul și persoana împuternicită de operator; d) capitolul V - Transferurile de date cu caracter personal către țări terțe sau organizații internaționale; e) capitolul VI - Autorități de supraveghere independente; f) capitolul VII - Cooperare și coerență; g) capitolul IX - Dispoziții referitoare la situații specifice de prelucrare. În același timp, Autoritatea națională de supraveghere a precizat că, potrivit considerentului (153) din preambulul

Regulamentului (UE) 2016/679, „Pentru a ține seama de importanța dreptului la libertatea de exprimare în fiecare societate democratică, este necesar ca noțiunile legate de această libertate, cum ar fi jurnalismul, să fie interpretate în sens larg”. De asemenea, a subliniat că persoanele care se consideră lezate din perspectiva unor prejudicii de imagine se pot adresa instanțelor de judecată în temeiul dispozițiilor Codului Civil.

CAPITOLUL V

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfășurării activității, potrivit Legii nr. 421/2023 a bugetului de stat pe anul 2024, Autorității naționale de supraveghere i s-a alocat un buget inițial pe anul 2024 în sumă de 5.990.000 lei, diminuat în urma aplicării prevederilor Ordonanțelor de Urgență ale Guvernului nr. 107/2024 pentru reglementarea unor măsuri fiscal-bugetare în domeniul gestionării creanţelor bugetare şi a deficitului bugetar pentru bugetul general consolidat al României în anul 2024, precum şi pentru modificarea şi completarea unor acte normative, cu modificările și completările ulterioare și nr. 113/2024 cu privire la rectificarea bugetului de stat pe anul 2024.

Ca atare, bugetul final pe anul 2024 al Autorității a fost în sumă de 5.714.000 lei și a avut următoarea structură:

- Cap. 51.01 Autorităţi executive și legislative – 5.714.000 lei
- Cheltuieli curente – 5.675.000 lei
- Titlul I Cheltuieli de personal – 4.634.000 lei
- Titlul II Bunuri şi servicii – 1.041.000 lei
- Cheltuieli de capital – 39.000 lei
- Titlul XIII Active nefinanciare – 39.000 lei

Creditele definitive aprobate au asigurat funcționarea instituției în anul 2024, în condiții de restricții bugetare, potrivit reglementărilor în vigoare.

Anul	2020	2021	2022	2023	2024
Buget final (mii lei)	4.903	4.601	5.580	5.595	5.714
% fata de anul anterior	95,26%	93,84%	121,27%	100,26%	102,13%

Bugetul anului 2024 a fost aproximativ la același nivel cu bugetul anului anterior, datorită restricțiilor bugetare stricte aplicate în semestrul II al anului 2024.

În faza de programare bugetară Autoritatea națională de supraveghere a avut în vedere obiectivele stabilite pentru anul 2024 și limitările bugetare transmise de Ministerul Finanțelor, pe baza cărora s-a fundamentat necesarul inițial de fonduri în sumă de 5.990.000 lei.

Evoluția macroeconomică pe anul 2024 a condus la impunerea de restricții și adoptarea de acte normative în urma cărora bugetul final al Autorității a scăzut la valoarea de 5.714.000 lei la 31 decembrie 2024.

În urma modificărilor de alocări bugetare realizate prin actele normative de rectificare a bugetului de stat pe anul 2024 și în urma anulărilor de credite realizate în luna decembrie 2024, potrivit reglementărilor Legii nr. 500/2002 privind finanţele publice, cu modificările și completările ulterioare, rezultă următoarea sinteză:

Denumire indicator	Cod	Buget iniţial 2024 - mii lei -	Buget final (actualizat la 31.12.2024) - mii lei -	Execuție bugetară la 31.12.2024 - mii lei -	Execuţie bugetară la 31.12.2024 (%)
Total cheltuieli	51.01	5.990	5.714	5.667,76	99,19
Titlul I Cheltuieli de personal	10	4.790	4.634	4.618,25	99,66
Titlul II Bunuri şi servicii	20	1.100	1.041	1.010,84	97,10
Cheltuieli de capital Titlul XIII Active nefinanciare	71	100	39	38,67	99,15

Menționăm faptul că în anul 2024 au fost recuperate sume din cheltuieli realizate în anii precedenți în valoare de 70.123,73 lei, acestea fiind transferate la bugetul de stat.

Precizăm că, în anul 2024, Autoritatea națională de supraveghere s-a confruntat, în continuare, cu o lipsă acută de personal, instituția desfășurându-și activitatea la finalul anului 2024 cu un număr de doar 34 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 2024 pentru un număr mediu de 34 de persoane (inclusiv demnitarii).

Numărul mediu de posturi ocupate în anul 2024 s-a menținut la același nivel cu anul 2023, în scădere față de media de 36 de posturi ocupate în anul 2022, și reprezintă un procent de doar 39% din numărul total de posturi prevăzut în legea de organizare (85 de posturi).

Angajarea cheltuielilor de personal s-a efectuat în baza prevederilor legale, respectiv:

- Legea nr. 102/2005 privind înființarea, organizarea şi funcţionarea Autorităţii Naţionale 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 bugetului de stat pe anul 2024 nr. 421/2023 și prevederile Ordonanțelor de Urgență ale Guvernului nr. 53, 107 și 113 din anul 2024, precum și prevederile aplicabile din Legea nr. 296/2023.

La titlul 20 "Bunuri şi servicii" sumele alocate prin buget au asigurat un minim necesar pentru desfășurarea activității Autorității naţionale de supraveghere.

Angajarea cheltuielilor cu bunuri și servicii a avut la bază actele şi documentele justificative, respectiv contracte de prestări servicii, achiziţii de bunuri, note de fundamentare aprobate de ordonatorul principal de credite şi s-a făcut în baza Legii nr. 98/2016 privind achizițiile publice și a celorlalte reglementări specifice, raportat și la restricțiile aplicabile în anul 2024 în ceea ce privește achizițiile (furnituri de birou, birotică, auto etc).

Pe parcursul anului 2024 o influență semnificativă asupra cheltuielilor cu bunuri și servicii au avut creșterile semnificative 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.

Menționăm faptul că, în anul 2024, au fost permanent ajustate necesitățile instituției privind cheltuielile cu bunuri și servicii (inclusiv cele pentru servicii și produse IT) și cheltuielile de investiții (active fixe corporale și necorporale), avându-se în vedere restricțiile bugetare impuse.

Potrivit reglementărilor legale în vigoare, evidența contabilă a fost ținută la zi, urmărindu-se legalitatea, oportunitatea și eficiența cheltuielilor bugetare, precum și încadrarea în creditele de angajament și în creditele bugetare alocate prin bugetul aprobat.

De asemenea, s-a avut în permanență în vedere respectarea limitelor lunare aprobate de Guvernul României și utilizarea sumelor alocate cu maximum de eficienţă posibilă într-o perioadă ce a continuat să fie influențată semnificativ de restricții bugetare.