ROMÂNIA
AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Bld.Gen. Gheorghe Magheru Nr. 28-30, Sector 1, Cod poştal 010336, Bucureşti ; Tel: +40.31.805.9211; Fax:+40.31.805.9602 www.dataprotection.ro; e-mail: anspdcp@dataprotection.ro

SEN
BIROUL PERMANENT
Nr. 1285
Data. 25.07.2022

Stimată Doamnă Preşedinte,

Am deosebita onoare de a supune atenţiei dumneavoastră Raportul de activitate aferent anului 2021, în conformitate cu dispoziţiile art. 5 din Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

Cu aleasă prețuire,

ROMÂNIA AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR

Preşedinte,

Ancuţa Gianina OPRE

Doamnei Alina-Ştefania GORGHIU
Preşedintele Senatului

SENATUL ROMÂNIEI

ANSPDCP Digitally signed by ANSPDCP
Date: 2022.07.19 09:21:

AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE

A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

RAPORT ANUAL

2021

Raportul de activitate este transmis Senatului României, Camerei Deputaţilor, Guvernului României, Comisiei Europene şi Comitetului European pentru Protecţia Datelor, în temeiul art. 5 din Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

Bucureşti

CUVÂNT ÎNAINTE

Stimate Domnule Preşedinte al Senatului,

Stimaţi Senatori,

Permiteți-mi să vă supun atenției principalele coordonate ale activității Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal în anul 2021, desfășurată sub corolarul protejării dreptului la viață privată și la protecția datelor cu caracter personal.

Acest an s-a înscris într-o perioadă de consolidare a aplicării reglementărilor europene în domeniul protecției datelor cu caracter personal, efect al aplicabilității directe, începând cu data de 25 mai 2018, a Regulamentului (UE) 2016/679 privind protecţia persoanelor fizice faţă de prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date şi de abrogare a Directivei 95/46/EC (Regulamentul General privind Protecția Datelor), adoptat de către Consiliu si Parlamentul European, dar și al aplicării celorlalte legi naționale în domeniu.

Aș dori să evidențiez că activitatea din anul 2021 a fost influențată inevitabil de efectele generate de evoluția pandemiei de Covid 19, ceea ce a antrenat, ca și anul anterior, o intensificare a interacțiunilor on-line. În acest context, remarcăm că au continuat eforturile operatorilor din mediul public si privat de aplicare a regulilor de utilizare a datelor personale, destinate respectării drepturilor persoanelor fizice și asigurării confidențialității și securității prelucrărilor de date personale, inclusiv prin modalitățile specifice mediului on-line.

Corelat cu rolul Autorității naționale de supraveghere de monitorizare și control al aplicării adecvate a regulilor de prelucrare a datelor personale, precum și de informare a publicului larg, menționăm că, în anul 2021, au continuat acțiunile de control la nivelul operatorilor din sectorul public și privat, din oficiu sau pe baza plângerilor și sesizărilor primite. În acest sens, menționăm că plângerile primite din partea persoanelor fizice au avut, în principal, ca obiect dezvăluirea neautorizată a datelor cu caracter personal, încălcarea drepturilor persoanelor vizate, nerespectarea principiilor de utilizare a datelor,

primirea de mesaje comerciale nesolicitate, încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale.

Reliefez cu acest prilej și continuarea activității Autorității de informare a publicului larg, cu privire la aplicarea adecvată a regulilor de utilizare a datelor cu caracter personal, adaptate la modalitățile particulare de desfășurare a acestora în special în mediul on-line, în contextul evoluțiilor pandemice ce au persistat în cursul anului 2021. Astfel, un instrument util l-au reprezentat comunicatele de presă care au reflectat măsurile adoptate și punctele de vedere ale instituției noastre, iar pentru a veni în sprijinul unor anumite categorii de operatori a fost pregătit și dat publicității Ghidul destinat clarificării modului de utilizare a datelor personale în activitatea asociațiilor de proprietari.

Raportat la obiectivele instituției noastre, în contextul pandemic al anului 2021, putem aprecia că acestea au fost îndeplinite cu toate că am dispus de resurse umane și financiare insuficiente.

Pe termen scurt, în perioada anilor 2022-2023, Autoritatea națională de supraveghere va urmări continuarea activității de monitorizare și control a operatorilor din sectorul public și privat, prin efectuarea de investigații din oficiu sau pe baza plângerilor primite, va continua activitățile de informarea publică a persoanelor fizice, operatorilor și mass-mediei, corelat cu mijloacele disponibile, în vederea determinării unei aplicări corespunzătoare a Regulamentului General privind Protecția Datelor și a celorlalte acte normative incidente.

În final, dați-mi voie să vă mulțumesc pentru sprijinul acordat instituției noastre și să-mi exprim încrederea că vom beneficia și pe viitor de susținerea Senatului României, în misiunea noastră de edificare a unei culturi în domeniul protecției datelor cu caracter personal în România.

Ancuța Gianina OPRE,

Președinte

CUPRINS

CAPITOLUL I
PREZENTARE GENERALĂ

Raportul de activitate pe anul 2021 al Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea națională de supraveghere) este structurat pe cinci capitole, astfel:

Capitolul I conține o prezentare sintetică pe principalele activități care se subsumează competențelor legale ale Autorității naționale de supraveghere, consacrate în principal prin prevederile următoarelor acte normative:

- Regulamentului (UE) 2016/679 al Parlamentului European și Consiliului 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) - denumit în continuare Regulamentul (UE) 2016/679,
- Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679,
- Legii nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date,
- Legii nr. 284/2018 privind utilizarea datelor din registrul cu numele pasagerilor din transportul aerian pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave, precum și pentru prevenirea și înlăturarea amenințărilor la adresa securității naționale,
- Legii nr. 141/2010 privind înființarea, organizarea și funcționarea Sistemului Informatic Național de Semnalări și participarea României la Sistemul de Informații Schengen,
- Legii nr. 271/2010 pentru înființarea, organizarea și funcționarea Sistemului național de informații privind vizele și participarea României la Sistemul de informații privind vizele,

- Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecţia vieţii private în domeniul comunicaţiilor electronice, cu modificările și completările ulterioare,

- Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

În cadrul **Capitolului al II-lea** sunt cuprinse informații sintetice și relevante referitoare la activitatea de reglementare, de avizare a proiectelor de acte normative, de autorizare şi de consiliere, precum şi la cea de informare publică, în conformitate cu sarcinile și competențele stabilite de Regulamentul (UE) 2016/679, precum și cu cele stabilite de celelalte acte normative în domeniu.

Această activitate s-a concretizat în emiterea avizelor asupra unui număr semnificativ de proiecte de acte normative şi de puncte de vedere referitoare la aplicarea adecvată a Regulamentului (UE) 2016/679 și a celorlalte reglementări incidente. Aceste opinii au urmărit furnizarea de informații către publicul larg în legătură cu exercitarea drepturilor lor în conformitate cu Regulamentul (UE) 2016/679 și îndeplinirea funcției de consiliere oferită autorităților sau instituțiilor publice ori altor entități.

Subliniem că, în anul 2021, atât persoanele fizice, cât 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, în special, informaţii cu privire la aplicabilitatea Regulamentului.

În secţiunea privind reprezentarea în faţa instanţelor de judecată sunt prezentate cele mai semnificative litigii finalizate pe parcursul anului 2021, în care a fost parte Autoritatea naţională de supraveghere, cu evidenţierea soluţiilor definitive pronunţate.

Secţiunea privind informarea publică expune principalele modalităţi de popularizare a regulilor de protecția datelor în cursul anului 2021, cu particularitățile specifice în contextul pandemiei de Covid 19 și raportat la limitele resurselor bugetare alocate.

Capitolul al III-lea constă într-o prezentare a principalelor aspecte din activitatea de control, în privinţa investigaţiilor din oficiu şi a celor efectuate pe baza plângerilor ori sesizărilor primite, inclusiv a datelor statistice relevante.

Investigaţiile efectuate din oficiu au avut ca obiect verificarea respectării prevederilor legale ca urmare, în special, a transmiterii notificărilor de încălcare a securității datelor cu

caracter personal, în aplicarea art. 33 alin. (1) din Regulamentul (UE) 2016/679, precum și ca urmare a sesizărilor transmise Autorității naționale de supraveghere. Referitor la incidentele de securitate, reliefăm faptul că acestea au vizat, în principal, aspecte privind confidențialitatea datelor cu caracter personal ca urmare a dezvăluirilor neautorizate, accesul neautorizat la sistemele de supraveghere video cu circuit închis și dezvăluirea de date cu caracter personal.

În ceea ce privește soluționarea plângerilor și a sesizărilor, în anul 2021 au continuat să fie sesizate, în principal, aspecte referitoare la încălcarea drepturilor și a principiilor prevăzute de Regulamentul (UE) 2016/679, dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate, prelucrarea imaginilor prin intermediul sistemelor de supraveghere video, primirea de mesaje comerciale nesolicitate, 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.

De asemenea, în cuprinsul acestui capitol sunt evidențiate măsurile corective dispuse în urma investigațiilor efectuate, inclusiv sancțiunile aplicate, dar și o serie de exemple în care au fost prezentate anumite cazuri investigate.

În cadrul investigaţiilor efectuate în anul 2021, au fost aplicate sancţiuni contravenţionale constând în amenzi în cuantum total de 371.132 lei.

Capitolul al IV-lea prezintă activitatea de relaţii externe a Autorităţii naţionale de supraveghere, prin sintetizarea diferitelor documente adoptate la nivelul Uniunii Europene, (cum ar fi orientări, avize, declarații), dar și a informațiilor privind transferul datelor în temeiul regulilor corporatiste obligatorii (BCR).

Totodată, sunt prezentate informații relevante privind cooperarea cu alte autorități de supraveghere din Uniunea Europeană în vederea asigurării asistenței reciproce, precum și informații utile referitoare la punctele de vedere emise de Autoritatea națională de supraveghere pe marginea documentelor primite.

Capitolul al V-lea conţine informaţii privind managementul economic al instituției, respectiv creditele bugetare puse la dispoziţia Autorităţii naţionale de supraveghere şi cheltuielile aferente.

Față de aspectele prezentate în cadrul fiecărui capitol, raportat la obiectivele Autorității naționale de supraveghere, rezultă că activitatea s-a desfășurat în condiții normale cu toate că resursele umane și financiare alocate instituției au fost insuficiente.

CAPITOLUL II
ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ŞI INFORMARE PUBLICĂ

Secțiunea 1
Activitatea de reglementare a Autorității naționale de supraveghere

Decizia nr. 20/2021 privind aprobarea Cerinţelor suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679 - Regulamentul General privind Protecția Datelor

Regulamentul (UE) 2016/679 prevede că statele membre, autoritățile naționale de supraveghere, Comitetul European privind Protecția Datelor și Comisia Europeană încurajează instituirea de mecanisme de certificare în domeniul protecției datelor, precum și de sigilii și mărci în acest domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă această reglementare, luându-se în considerare necesitățile specifice ale microîntreprinderilor, ale întreprinderilor mici și mijlocii.

În cursul anului 2021, în considerarea prevederilor articolelor 42 - 43 din Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere a emis Decizia nr. 20/2021 privind aprobarea Cerințelor suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679.

Menționăm, în acest context, că art. 43 din Regulamentul (UE) 2016/679 dispune că statele membre se asigură că organismele de certificare pot fi acreditate de organismul național de acreditare desemnat în conformitate cu Regulamentul (CE) nr. 765/2008 al Parlamentului European și al Consiliului, în conformitate cu standardul EN-ISO/IEC 17065/2012 și cu cerințele suplimentare stabilite de Autoritatea națională de supraveghere.

Astfel, în urma consultărilor avute cu organismul de certificare din România – Asociația de Acreditare din România (RENAR) și având în vedere documentul emis de Comitetul European pentru Protecția Datelor intitulat "Orientările nr. 1/2018 privind

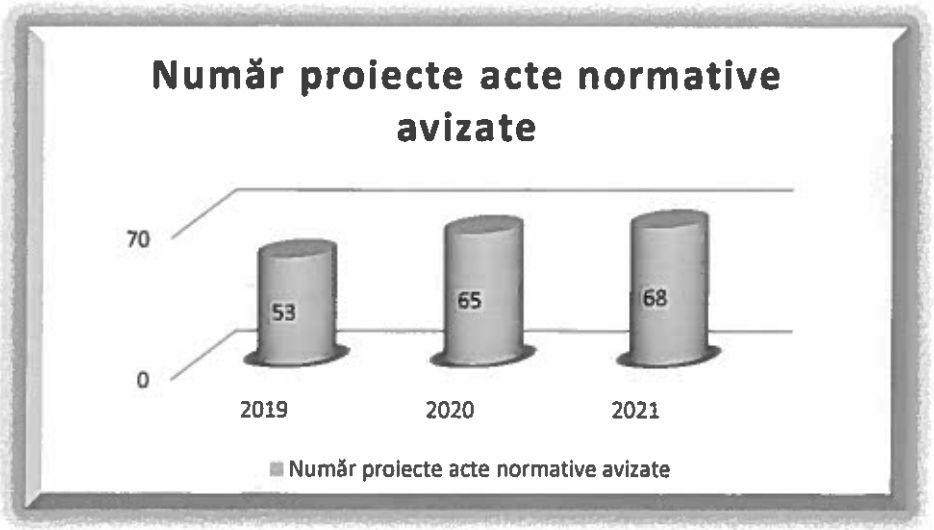
certificarea şi identificarea criteriilor de certificare în conformitate cu articolele 42 și 43 din Regulamentul general privind protecția datelor" din 4 iunie 2019, la nivelul Autorității naționale de supraveghere au fost elaborate cerințele suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679.

Decizia nr. 20/2021, intrată în vigoare la data de 12 iulie 2021, conține cerințele necesare care să permită acreditarea, ce au fost structurate în capitolele IV-IX și vizează cerințe generale privind acreditarea, cerințe referitoare la structură, la resurse, cerințe referitoare la proces, la sistemul de management și alte cerințe suplimentare, raportate inclusiv la standardul european ENISO/IEC 17065/2012.

Totodată, menționăm că Asociația de Acreditare din România – RENAR, în calitate de organism național de acreditare, în conformitate cu Regulamentul (CE) nr. 765/2008 și Ordonanţa Guvernului nr. 23/2009 privind activitatea de acreditare a organismelor de evaluare a conformității, cu modificările și completările ulterioare, urmează să pună în aplicare dispozițiile art. 11 din Legea nr. 190/2018, pe baza criteriilor stabilite prin Decizia nr. 20/2021.

Secțiunea a 2-a: Avizarea actelor normative

În anul 2021, Autoritatea naţională de supraveghere a emis avize asupra unui număr de **68 de proiecte de acte normative** elaborate de instituţii şi autorităţi publice care implicau aspecte complexe privind prelucrarea datelor cu caracter personal, în temeiul art. 57 alin. (1) lit. c) din Regulamentul (UE) 2016/679.



Proiectele de acte normative au fost transmise de către unele ministere, precum Ministerul Afacerilor Interne, Ministerul Muncii și Solidarității Sociale, Ministerul Dezvoltării, Lucrărilor Publice și Administrației, Ministerul Agriculturii și Dezvoltării Rurale, Ministerul Transporturilor și Infrastructurii, Ministerul Comunicațiilor și Societății Informaționale, Ministerul Finanțelor, Ministerul Mediului, Apelor și Pădurilor, Ministerul Afacerilor Externe, Ministerul Sănătății, Ministerul Educației, Ministerul Investițiilor și Proiectelor Europene dar și de către alte autorități sau instituții publice centrale, cum ar fi: Autoritatea Electorală Permanentă, Institutul Național de Statistică, Agenția Națională Anti-Doping, Agenția Națională a Funcționarilor Publici.

De asemenea, Secretariatul General al Guvernului - Departamentul pentru Relația cu Parlamentul a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la diferite propuneri legislative.

În majoritatea cazurilor, Autoritatea națională de supraveghere a apreciat că este necesară completarea sau modificarea textelor respective, efectuând o serie de observații și propuneri, prin raportare la necesitatea armonizării unor dispoziții din proiectele sau propunerile respective cu principiile și condițiile de prelucrare a datelor cu caracter personal.

În continuare, prezentăm unele dintre cele mai importante proiecte de acte normative avizate:

► **Ministerul Afacerilor Interne a solicitat exprimarea unui punct de vedere cu privire la *proiectul de Lege privind organizarea și funcționarea Sistemului Informatic Național de Semnalări și participarea României la Sistemul de Informații Schengen, precum și pentru modificarea și completarea unor acte normative.***

Prin proiectul de act normativ supus atenției Autorității naționale de supraveghere sunt stabilite măsurile necesare punerii în aplicare la nivel național a prevederilor cuprinse în Regulamentul (UE) 2018/1860 privind utilizarea Sistemului de informații Schengen pentru returnarea resortisanților țărilor terțe aflați în situație de ședere ilegală, în Regulamentul (UE) 2018/1861 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere, de modificare a Convenției de punere în aplicare

a Acordului Schengen şi de modificare şi abrogare a Regulamentului (CE) nr. 1987/2006, precum și cele cuprinse în Regulamentul (UE) 2018/1862 privind instituirea, funcţionarea şi utilizarea Sistemului de informaţii Schengen (SIS) în domeniul cooperării poliţieneşti şi al cooperării judiciare în materie penală, de modificare şi de abrogare a Deciziei 2007/533/JAI a Consiliului şi de abrogare a Regulamentului (CE) nr. 1986/2006 al Parlamentului European şi al Consiliului şi a Deciziei 2010/261/UE a Comisiei.

Având în vedere conținutul proiectului de lege analizat, au fost făcute următoarele observații și propuneri:

Autoritatea națională de supraveghere a propus reanalizarea în vederea completării anumitor prevederi, prin raportare la definițiile din Regulamentul (UE) 2018/1860, Regulamentul (UE) 2018/1861 şi Regulamentul (UE) 2018/1862 (de ex. definiția *"semnalării"* din art. 2 alin. (2) lit. k) din proiect nu corespunde definiției semnalării din cele trei regulamente invocate; în proiect nu se regăsesc, printre altele, definițiile termenilor de "date cu caracter personal", "prelucrare de date cu caracter personal", "date biometrice", "date dactiloscopice", "imagine facială").

De asemenea, s-a considerat că este necesară reanalizarea art. 6 alin. (3) din proiect prin care se stabilește dreptul de acces la SINS în acord cu prevederile art. 17 din Regulamentul (UE) 2018/1860, art. 34 din Regulamentul (UE) 2018/1861, precum şi art. 44 din Regulamentul (UE) 2018/1862, care conțin și dispoziții referitoare la dreptul autorităților competente "de a efectua căutări în aceste date în mod direct sau într-o copie a bazei de date SIS".

Referitor la art. 9 alin. (1) lit. e) din proiect s-a subliniat că acesta nu este în concordanță cu prevederile art. 32 alin. (1) lit. d) pct. (i) din Regulamentul (UE) 2018/1862. De asemenea, Autoritatea națională de supraveghere a solicitat reanalizarea art. 34 alin. (2) din proiect întrucât conținutul acestuia este neclar.

Cât privește art. 60 alin. (1) din proiect s-a considerat că este necesară reanalizarea acestuia în concordanță cu prevederile invocate din Regulamentul (UE) 2018/1860, Regulamentul (UE) 2018/1861 şi Regulamentul (UE) 2018/1862 sens în care se impune realizarea "unui inventar actualizat" a copiilor tehnice realizate. În acord cu aceleași reglementări europene invocate în art. 60 alin. (1) din proiect, s-a specificat că trebuie pus la dispoziția Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal inventarul actualizat a copiilor tehnice realizate de autoritățile competente.

Autoritatea națională de supraveghere a considerat, referitor la alt articol din proiectul de act normativ, că este necesară punerea prevederilor acestuia în deplin acord cu dispozițiile art. 45 alin. (3) din Regulamentul (UE) 2018/1861, precum și cu dispozițiile art. 60 alin. (3) din Regulamentul (UE) 2018/1862, inclusiv în ceea ce privește menționarea tuturor autorităților către care Centrul Național SIS are obligația de a notifica incidentele de securitate.

Referitor la dispozițiile art. 69 alin. (4) din proiect, pentru claritatea textului normativ, s-a apreciat că este necesară completarea acestuia cu trimiterea și la art. 10 alin. (1) - (3) și în cazul Regulamentului (UE) 2018/1862.

Autoritatea națională de supraveghere a mai recomandat reanalizarea dispozițiilor art. 71 alin. (2) din proiect, în vederea completării articolului sub aspectul introducerii în cuprinsul său a excepțiilor la care se face referire în art. 12 alin. (1) din Regulamentul (UE) 2018/1861, respectiv în art. 12 alin. (1) din Regulamentul (UE) 2018/1862.

Autoritatea națională de supraveghere a considerat, în ceea ce privește Secțiunea a 5-a "Protecția persoanelor cu privire la prelucrarea datelor cu caracter personal" din proiectul de lege analizat, că este necesară introducerea unui articol distinct, în acord cu dispozițiile art. 51 alin. (2) din Regulamentul (UE) 2018/1861 și cu dispozițiile art. 66 alin. (2) și (3) din Regulamentul (UE) 2018/1862, în care să se prevadă că prelucrările de date cu caracter personal efectuate în aplicarea dispoziţiilor Legii privind organizarea şi funcţionarea Sistemului Informatic Naţional de Semnalări şi participarea României la Sistemul de Informaţii Schengen, precum şi pentru modificarea şi completarea unor acte normative, se fac cu respectarea prevederilor Regulamentului (UE) 2016/679, respectiv a 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 prelucrarea datelor cu caracter personal.

În același timp, s-a considerat că textul proiectului ar trebui să fie completat astfel încât să conțină prevederi distincte cu privire la informarea persoanei vizate despre posibilitatea de a depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal sau de a introduce o cale de atac judiciară.

De asemenea, s-a solicitat reanalizarea conținutului art. 77 alin. (2) din proiect și a propus completarea prevederilor acestuia în sensul că auditarea operațiunilor de prelucrare în N.SIS fie se efectuează de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, fie aceasta dispune în mod direct efectuarea auditului de un auditor independent în materie de protecţie a datelor, cu păstrarea în permanenţă a controlului asupra auditorului independent şi asumarea responsabilităţile acestuia, în conformitate cu dispozițiile art. 55 alin. (2) din Regulamentul (UE) 2018/1861 și art. 69 alin. (2) din Regulamentul (UE) 2018/1862.

Prin urmare, Autoritatea națională de supraveghere a considerat că este necesară reanalizarea integrală a proiectului de Lege transmis, pentru a asigura concordanța cu Regulamentele invocate.

► **Ministerul Muncii și Solidarității Sociale a solicitat exprimarea unui punct de vedere cu privire la *proiectul de Ordonanță de Urgență a Guvernului pentru stabilirea unor măsuri de protecție socială a angajaților și a altor categorii profesionale în contextul interzicerii, suspendării ori limitării activităților economice, determinate de situaţia epidemiologică generată de răspândirea coronavirusului SARS-CoV-2, precum și pentru modificarea unor acte normative.***

Autoritatea națională de supraveghere a formulat o serie de observații și propuneri, astfel:

În ceea ce privește modelele de cereri și documente prevăzute de acest proiect de ordonanță, necesar a fi completate de către salariaţi pe perioada reducerii sau întreruperii temporare a activității total sau parțial, ca urmare a implementării măsurilor pentru diminuarea impactului tipului de risc prevăzute de hotărârile Guvernului pentru prelungirea stării de alertă pe teritoriul României, în vederea acordării indemnizației, s-a recomandat să fie luat în considerare faptul că angajatorii trebuie să colecteze și prelucreze de la aceștia doar datele adecvate, relevante și limitate la ceea ce este necesar în raport de scopul prelucrării.

Cu privire la dispozițiile referitoare la transmiterea de date cu caracter personal între Agenția Națională pentru Ocuparea Forței de Muncă și Agenția Națională pentru Plăți și Inspecție Socială, în baza unui protocol încheiat între aceste entități, s-a evidențiat hotărârea Curții de Justiție a Uniunii Europene care, în Cauza Bara împotriva României C-201/14, în

ceea ce privește baza legală a transmiterii unor date personale între diverse entități publice, statuează că *"modalitățile de efectuare a transmiterii acestor informații au fost elaborate nu prin intermediul unei măsuri legislative, ci prin intermediul Protocolului din 2007 încheiat între ANAF și CNAS, care nu ar fi făcut obiectul unei publicări oficiale."* (pct. 40).

Ca atare, s-a solicitat modificarea acestor dispoziții din proiect în sensul înlocuirii sintagmei "protocol" cu cea de "act administrativ cu caracter normativ", raportat la necesitatea asigurării principiului transparenței stabilit de art. 12 din RGPD.

► **Ministerul Sănătății a solicitat exprimarea unui punct de vedere cu privire la *proiectul de Ordonanță a Guvernului pentru modificarea și completarea Legii nr. 95/2006 privind reforma în domeniul sănătății.***

Autoritatea națională de supraveghere a recomandat modificarea textului proiectului în sensul următoarelor observații:

Față de prevederile pct. 14 din proiectul de act normativ supus analizei, s-a propus completarea textului art. 108 alin. (13) și cu mențiuni referitoare la colectarea datelor cu respectarea Regulamentului (UE) 2016/679, precum și a legislației naționale aplicabile domeniului protecției datelor. Aceeași observație a fost formulată și în legătură cu dispozițiile pct. 52 din proiect, prin s-a propus completarea textului art. 944 alin. (2) din Legea nr. 95/2006.

De asemenea, având în vedere dispozițiile ART. III din proiect, s-a solicitat reformularea acestuia în sensul că sintagma „Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare" să se înlocuiească cu sintagma „Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor – RGPD), precum și legislația națională aplicabilă domeniului protecției datelor", raportat la prevederile art. V din Legea nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, republicată.

► **Ministerul Transporturilor și Infrastructurii a solicitat avizul Autorității naționale de supraveghere cu privire la *proiectul de Ordonanță a Guvernului privind interoperabilitatea sistemelor de tarifare rutieră electronică și facilitarea schimbului transfrontalier de informații cu privire la neplata tarifelor rutiere.***

Având în vedere unele observații anterioare ale Autorității naționale de supraveghere asupra proiectului de act normativ analizat, acesta a fost refăcut parțial de către inițiator însă fără a se ține cont de toate observațiile efectuate, raportat la domeniul protecției datelor cu caracter personal.

Ca atare, Autoritatea națională de supraveghere și-a menținut observațiile nepreluate, întrucât a considerat ca fiind necesară o transpunere corectă a Directivei 2019/520 privind interoperabilitatea sistemelor de taxare rutieră electronică şi facilitarea schimbului transfrontalier de informaţii cu privire la neplata taxelor rutiere în cadrul Uniunii.

În acest sens, s-a menținut observația referitoare la art. 14 alin. (2) din Directiva anterior menționată, care vizează faptul că furnizorii de servicii de taxare, inclusiv furnizorii SETRE trebuie să prezinte, la cererea autorităților statelor membre, date referitoare la clienții lor, cu condiția să fie respectate normele aplicabile în materie de protecție a datelor.

De asemenea, s-a reiterat observația privind art. 27 alin. (2) lit. c (c) teza a II-a din Directiva 2019/520, sub aspectul stabilirii măsurilor necesare pentru asigurarea drepturilor persoanelor vizate de către operatorii implicați, a dreptului de a depune o plângere la Autoritatea națională de supraveghere, de compensare și de acces la o cale de atac eficace.

► **Ministerul Investițiilor și Proiectelor Europene a solicitat exprimarea unui punct de vedere cu privire la *proiectul de Hotărâre a Guvernului privind aprobarea unor măsuri pentru acordarea unui sprijin material pe bază de tichete sociale pe suport electronic pentru nou-născuți finanțate din fonduri externe nerambursabile, precum și unele măsuri de distribuire a acestora.***

Autoritatea națională de supraveghere a apreciat, față de art. 6 alin. (1) din proiect, că este necesară eliminarea înscrierii pe tichetul social a "codului numeric personal al destinatarului final eligibil și al noului-născut", raportat la scopul prelucrării, respectiv, acordarea unui sprijin material pe bază de tichete sociale pe suport electronic pentru nou-născuți, finanțate din fonduri externe nerambursabile, pentru respectarea principiului

proporționalității prelucrării de date personale, statuat în art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679.

În același timp, Autoritatea națională de supraveghere a propus modificarea alin. (11) al art. 6 din proiect în sensul că toate entitățile implicate în implementarea programului sunt obligate să respecte Regulamentul (UE) 2016/679 precum și celelalte reglementări din domeniul protecției datelor.

► **Agenția Națională a Funcționarilor Publici a solicitat exprimarea unui punct de vedere cu privire la *proiectul de Hotărâre a Guvernului privind conținutul și modalitatea de gestionare a dosarului profesional al funcționarilor publici.***

Autoritatea națională de supraveghere a făcut o serie de observații și propuneri, raportat la conținutul proiectului supus atenției, astfel:

S-a solicitat reevaluarea termenelor de depunere a cererii și documentelor necesare în vederea acordării unor indemnizații, în format electronic, la agenţiile pentru plăţi şi inspecţie socială judeţene, respectiv a municipiului Bucureşti, raportat la prevederile art. 12 alin. (3) și art. 15 din RGPD.

De asemenea, s-a apreciat ca fiind necesară reformularea unor dispoziții din proiect în sensul în care toate entitățile care aplică dispozițiile acestei hotărâri, inclusiv Agenția Națională a Funcționarilor Publici, au obligația să respecte prevederile Regulamentului (UE) 2016/679, precum și celelalte reglementări aplicabile din domeniul protecției datelor personale.

În consecință, s-a solicitat reanalizarea proiectului de Hotărâre a Guvernului supus atenției Autorității naționale de supraveghere, prin raportare la aspectele prezentate.

Ulterior, Agenția Națională a Funcționarilor Publici a retransmis proiectul de Hotărâre a Guvernului, modificat corespunzător.

► **Ministerul Sănătății a supus avizării Autorității naționale de supraveghere *proiectul Ordonanței Guvernului pentru modificarea și completarea Legii nr. 55/2020 privind unele măsuri pentru prevenirea și combaterea efectelor pandemiei de COVID-19.***

Autoritatea națională de supraveghere a formulat observații și propuneri în ceea ce privește textul proiectului de act normativ.

Astfel, având în vedere faptul că datele privind vaccinarea unei persoane fizice reprezintă date privind starea de sănătate și se supun condițiilor de prelucrare prevăzute la art. 9 din Regulamentul (UE) 2016/679, s-a precizat că, în jurisprudența sa (Decizia nr. 498/2018 asupra dispozițiilor din Legea nr. 95/2006 referitoare la Dosarul Electronic de Sănătate), Curtea Constituțională a subliniat necesitatea unui nivel înalt de protecţie a datelor cu caracter medical, legiuitorul având obligaţia de a reglementa garanţiile asociate dreptului la viaţă intimă, familială şi privată prin lege, în sens de instrumentum.

Autoritatea națională de supraveghere a subliniat faptul că dispozițiile proiectului Ordonanței Guvernului trebuie să cuprindă nu doar temeiul legal al prelucrării datelor privind starea de sănătate, ci trebuie să asigure și o protecţie specifică a datelor medicale, prin stabilirea unor garanţii care să ateste nivelul adecvat de protecţie a datelor cu caracter medical.

În consecință, s-a subliniat faptul că este necesar ca în textul proiectului de ordonanță (iar nu într-un ordin de ministru) să fie reglementate următoarele aspecte: tipurile de date care fac obiectul prelucrării, entităţile cărora le pot fi divulgate datele şi scopul pentru care respectivele date cu caracter personal pot fi divulgate, limitările legate de scop și perioadele de stocare.

Autoritatea națională de supraveghere a semnalat, raportat la prevederile art. 5 alin. (2), art. 24 și art. 32 din RGPD, faptul că textul proiectului de ordonanță trebuie să identifice cu claritate entitățile care au calitatea de operatori/operatori asociați/împuterniciți și, implicit, poartă răspunderea în ceea ce privește prelucrarea datelor personale în cadrul activității reglementate de proiect (acordarea tichetelor de masă și Loteria de vaccinare), inclusiv sub aspectul măsurilor tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului.

În același timp, raportat la propunerea de acordare a tichetelor de masă, s-a subliniat că este necesară clarificarea temeiului legal al prelucrării datelor preconizate la art. 21 ind. 2 din proiect, de către angajatori, precum și identificarea clară a datelor ce vor fi prelucrate, având în vedere că se prelucrează informații privind starea de sănătate a angajatului, date pe care angajatorii nu le pot prelucra decât cu respectarea condițiilor prevăzute la art. 9 alin. (2) din RGPD.

► **Ministerul Muncii și Protecției Sociale a solicitat exprimarea unui punct de vedere cu privire la *proiectul de Lege privind stabilirea măsurilor de protecție socială pentru consumatorul vulnerabil de energie.***

Față de conținutul proiectului supus atenției Autorității naționale de supraveghere, prin raportare la dispozițiile Regulamentului (UE) 2016/679, au fost formulate următoarele observații și propuneri:

În contextul dispozițiilor art. 4 alin. (4) din proiectul de lege referitoare la categoria consumatorilor vulnerabili din motive de sănătate, s-a precizat faptul că art. 9 din RGPD prevede că datele cu caracter special (categorie din care fac parte și datele privind starea de sănătate) se prelucrează cu consimțământul explicit al persoanelor vizate.

Ca atare, s-a considerat necesară introducerea în proiectul de lege a unor prevederi în sensul obținerii consimțământului consumatorilor vulnerabili din motive de sănătate pentru prelucrarea datelor privind starea de sănătate a acestora, cu respectarea principiului transparenței prevăzut în art. 13, respectiv art. 14 din RGPD.

În legătură cu prevederea din art. 14 alin. (5) din proiectul de act normativ supus analizei, s-au reiterat cele statuate de CJUE în cauza C-201/14 (*Smaranda Bara și alții)*, în ceea ce privește baza legală a transmiterii unor date personale între diverse entități publice.

În sensul celor precizate, întrucât este necesară asigurarea respectării principiului transparenței statuat de art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679, coroborat cu jurisprudența CJUE, Autoritatea națională de supraveghere a propus modificarea textului în discuție, prin eliminarea sintagmei "protocol" și înlocuirea acesteia cu "act administrativ cu caracter normativ".

În ceea ce privește art. 17 alin. (3) din proiectul de lege care prevede transmiterea, atât în format electronic cât și scris, de către primari către agenții teritoriale, furnizori de energie termică în sistem centralizat, de gaze naturale/energie electrică și asociații de proprietari/locatari, a situațiilor centralizatoare privind titularii ajutoarelor, situații care conțin "și venitul net lunar pe membru de familie și valoarea ajutorului (...)" , așadar o serie de date cu caracter personal printre care și cele menționate anterior, s-a atras atenția asupra faptului că o astfel de dezvăluire a datelor prezintă riscul ca acestea să devină accesibile unui număr nedefinit de persoane, cu o potențială utilizare ulterioară neconformă cu dispozițiile legale privind protecția datelor și cu riscul aducerii unor atingeri grave drepturilor și libertăților fundamentale ale persoanelor fizice.

În sensul celor de mai sus, s-a considerat că este necesar ca în textul proiectului de act normativ să se specifice care sunt datele cu caracter personal adecvate și relevante și să se limiteze acele date ce urmează a fi comunicate, pentru a se evita o eventuală ingerință în viața privată a persoanelor fizice, pentru respectarea principiului caracterului adecvat al datelor, precum și a obligațiilor de confidențialitate și securitate a datelor cu caracter personal, în acord cu prevederile art. 5 și art. 32 RGPD.

Autoritatea națională de supraveghre a considerat că este necesară modificarea art. 39 alin. (2) din textul proiectului de lege, astfel încât în cuprinsul acestuia să se menționeze că entitățile care prelucrează date cu caracter personal, în aplicarea dispoziţiilor referitoare la stabilirea măsurilor de protecție socială pentru consumatorul vulnerabil de energie, efectuează aceste prelucrări cu respectarea prevederilor Regulamentului (UE) 2016/679, inclusiv în ceea ce privește confidențialitatea și securitatea datelor.

În consecință, s-a considerat că proiectul de lege supus atenției Autorității naționale de supraveghere trebuie reanalizat sub toate aspectele puse în discuție.

► **Secretariatului General al Guvernului a transmis solicitarea de exprimare a unei opinii în vederea susținerii sau respingerii *propunerii legislative privind stabilirea anumitor prevederi referitoare la certificarea istoricului vehiculelor rutiere utilizate în vederea înmatriculării acestora în România (Bp. 522/2021)*.**

Având în vedere conținutul propunerii supuse atenției Autorității naționale de supraveghere, prin raportare la dispozițiile Regulamentului (UE) 2016/679, s-a subliniat faptul că activităţile desfăşurate în legătură certificarea istoricului vehiculelor rutiere utilizate în vederea înmatriculării acestora în România, așa cum se regăsesc în propunerea legislativă, presupun efectuarea de operaţiuni de prelucrare de date cu caracter personal, care trebuie să respecte principiile de prelucrare prevăzute în Regulament.

Prin urmare, Autoritatea națională de supraveghere a arătat necesitatea luării în considerare a dispozițiilor art. 5, art. 6 și art. 9, coroborate cu art. 24 și art. 25 din RGPD.

În acest context, s-a subliniat faptul că, din conținutul propunerii, nu reiese cu claritate care sunt datele cu caracter personal care urmează a fi prelucrate (de ex. colectate, înregistrate, organizate, structurate, stocate, consultate, utilizate, divulgate prin transmitere); în tot cuprinsul propunerii se face referire la "informații" "prelevate" de

"Registrul Auto Român" sau "transmise" de diverse entități precum, "ateliere autorizate" „operatorii economici autorizați" (art. 1, art. 3, art. 4 din propunere).

Raportat la textul propunerii s-a precizat faptul că este necesară stabilirea calității de operator, respectiv de împuternicit (conform definițiilor acestor noțiuni din RGPD) a entității/entităților, după caz, care va gestiona/administra registrul înființat potrivit art. 1 alin. (1) din propunere, respectiv a celor care vor prelucra date pentru certificarea istoricului vehiculelor rutiere.

Autoritatea națională de supraveghere a atras atenția asupra responsabilității operatorului (art. 24 RGPD), precum și a faptului că art. 25 RGPD stabilește că este necesară asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit, respectiv asigurarea principiilor privacy by design și by default.

Prin urmare, s-a considerat necesar să fie prevăzut în propunerea legislativă faptul că sistemul de evidență care va asigura colectarea, înregistrarea și stocarea datelor personale în contextul certificării istoricului vehiculelor rutiere, trebuie să fie constituit în concordanță cu principiile stabilite de RGPD, să asigure și să respecte standarde de securitate şi de confidenţialitate adecvate pentru protejarea datelor.

Autoritatea națională de supraveghere a propus inserarea unor prevederi referitoare la protecţia datelor împotriva prelucrării neautorizate sau ilegale, precum şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare ("integritate şi confidenţialitate") de către toate entitățile implicate în certificarea istoricului vehiculelor rutiere.

Prin urmare, față de cele anterior expuse, Autoritatea națională de supraveghere a recomandat reanalizarea propunerii de act normativ, sub aspectul celor prezentate anterior.

► **Ministerul Afacerilor Interne a solicitat exprimarea unui punct de vedere cu privire la conținutul *propunerilor de acte normative europene care fac parte din pachetul de propuneri privind un Cod de Cooperare Polițienească.***

Autoritatea națională de supraveghere nu a avut observații față de propunerea de Recomandare a Consiliului privind cooperarea polițienească operativă (COM/2021/780 final), având în vedere faptul că în Memorandumul explicativ al acesteia se precizează, în ceea ce privește protecția datelor cu caracter personal, că vor fi respectate dispozițiile Directivei 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.

În ceea ce privește proiectul de Directivă a Parlamentului European și a Consiliului privind schimbul de informații între autoritățile de aplicare a legii din statele membre (COM/2021/782 final), este menționat considerentul (16) în care se prevede că regulile stabilite în acesta trebuie să fie puse în acord, cu precădere în ceea ce privește principiile de prelucrare a datelor cu caracter personal, cu Directiva 680/2016 și Regulamentul (UE) 2016/679.

Prin urmare, în considerarea celor de mai sus, raportat la proiectul de directivă analizat, Autoritatea națională de supraveghere a apreciat că este necesară:

- clarificarea dispozițiilor art. 3 lit. (a) din proiect care fac referire la "orice informații relevante" ("any relevant information");

- detalierea prevederilor art. 4 din proiect, în sensul menționării în mod expres a categoriilor de date care urmează să facă obiectul schimbului de informații realizat prin intermediul punctului unic de contact desemnat în fiecare stat membru.

Referitor la proiectul de Regulament a Parlamentului European și a Consiliului privind schimbul automat de date în scopul cooperării polițienești Prüm II (COM/2021/784 final), Autoritatea națională de supraveghere a atras atenția asupra următoarelor aspecte:

- definițiile noțiunilor de imagine facială și date biometrice (art. 4 pct. 10 și 11) nu sunt în acord cu definiția datelor biometrice din Regulamentul (UE) 2016/679 și Directiva 680/2016;

- cu privire la art. 33 ("Justification for the processing of data") s-a considerat că este necesară clarificarea termenului de "justificare";

- în art. 51 alin. (3) se menționează că datele vor fi șterse imediat, cu excepția situației în care prelucrarea lor este necesară în scop de prevenire, detectare și investigare, iar în art. 51 alin. (4) se menționează că datele vor fi șterse imediat, cu excepția situației în care prelucrarea lor este necesară pentru înregistrarea prevăzuta la art. 20 din propunere; s-a apreciat că este necesară clarificarea diferenței între cele două dispoziții;

- referitor la prevederile art. 52 alin. (1) s-a considerat că este util să se precizeze în mod expres cine este responsabil cu rectificarea, respectiv cu ștergerea datelor, precum și

să se specifice care dintre părți va rectifica/șterge datele, cu informarea/acordul statului membru care a introdus datele;

- cu privire la dispozițiile art. 52 alin. (2) s-a apreciat că sunt necesare clarificări cu privire la semnalizarea datelor aflate în posesia unui stat membru dar a căror acuratețe este contestă de persoana vizată, în sensul dacă datele "marcate" vor fi prelucrate în continuare;

- referitor la art. 52 alin. (3) lit. b), pentru armonizarea prevederii la nivelul statelor membre, s-a recomandat stabilirea unei perioade maxime de păstrare a datelor, aplicabilă tuturor statelor membre;

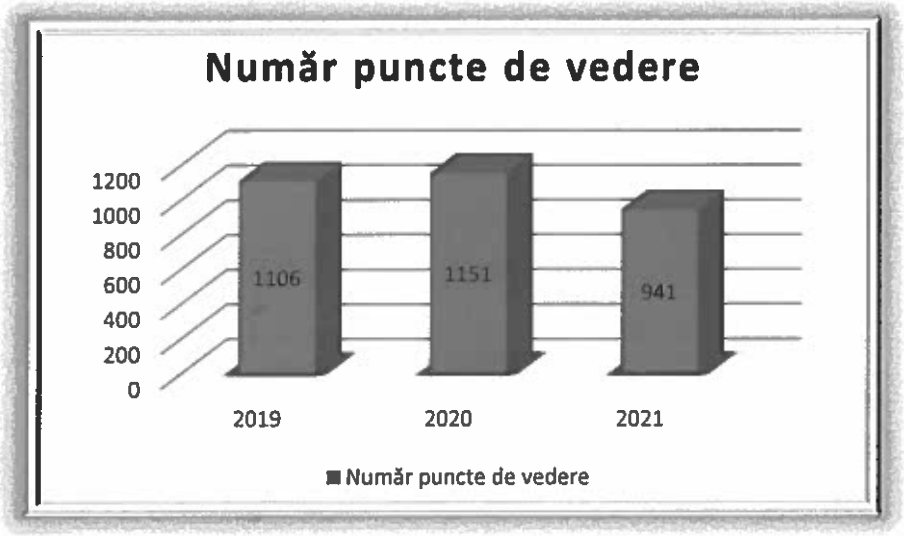
- s-a considerat necesară completarea textului art. 55 alin. (3) cu sintagma "(...) in any event no later than (...)" și stabilirea unui termen limită de notificare către autoritățile de supraveghere compente.

Autoritatea națională de supraveghere a considerat că este necesară includerea în proiectul de regulament a unor dispoziții referitoare la drepturile persoanelor vizate.

Secțiunea a 3 – a:
Puncte de vedere privind diverse chestiuni de protecţia datelor

Pe parcursul anului 2021 a fost adresat Autorității naţionale de supraveghere un număr de **941 solicitări** de emitere puncte de vedere privind diverse aspecte referitoare la modalitatea de interpretare și aplicare a Regulamentului (UE) 2016/679, de către operatori și împuterniciții acestora, din domeniul public și privat, de către alte entități, precum și de către persoane fizice.

Având în vedere prelungirea contextului pandemic, se poate observa menținerea în 2021 a unui număr semnificativ de solicitări, ceea ce demonstrează interesul manifestat în ceea ce privește asigurarea respectării regulilor de prelucrare a datelor personale instituite de Regulamentul (UE) 2016/679 și legislația națională conexă.



▪ **Prezentăm în continuare unele dintre cazurile semnificative supuse atenției Autorității naționale de supraveghere, astfel:**

► ***Prelucrarea unor categorii speciale de date cu caracter personal de către o companie multinațională***

O societate de avocatură a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la unele aspecte legate de prelucrarea de categorii speciale de date cu caracter personal de către o companie multinațională care dorește să implementeze un program de diversitate și incluziune pentru angajații săi din întreaga lume, inclusiv din România.

În considerarea celor descrise în adresa transmisă, Autoritatea națională de supraveghere a precizat, în ceea ce privește prelucrarea datelor privind orientarea sexuală, identitatea de gen, dizabilitatea și originea etnică, care fac parte din categoria datelor speciale, că aceasta se supune condițiilor prevăzute de art. 9 din Regulamentul (UE) 2016/679 (RGPD).

S-a subliniat că este necesară respectarea condițiilor prevăzute de art. 7 coroborat cu art. 4 pct. (32) din RGPD, ținând cont și de recomandările din documentul intitulat "Orientări asupra Consimțământului în temeiul Regulamentului 2016/679" (WP 259) emis de fostul Grup de Lucru Art. 29 (în prezent Comitetul european pentru protecția datelor).

În plus, considerentul (42) din RGPD statuează: "Consimţământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimţământul fără a fi prejudiciată."

În aceleași "Orientări asupra Consimțământului în temeiul Regulamentului 2016/679" se menționează următoarele:

"Cu toate acestea, în cadrul cerințelor RGPD, operatorii au libertatea de a elabora un flux de lucru privind consimțământul care să se potrivească organizației lor (...).

Operatorii ar trebui să elaboreze mecanisme de consimțământ clare pentru persoanele vizate. Operatorii trebuie să evite ambiguitatea și trebuie să se asigure că acțiunea prin care este acordat consimțământul se poate deosebi de alte acțiuni (...).

De exemplu, în contextul digital sau on-line, persoana vizată poate să dea declarația solicitată prin completarea unui formular electronic, prin trimiterea unui e-mail, prin încărcarea unui document scanat care poartă semnătura persoanei vizate sau prin utilizarea unui semnături electronice (...)."

Cât privește consimțământul angajatului, Autoritatea națională de supraveghere a precizat că fostul Grup de Lucru art. 29 menționează în documentul intitulat "Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă" faptul că: "Angajații nu sunt aproape niciodată în măsură să își exprime, să refuze sau să își revoce în mod liber consimțământul, având în vedere dependența care rezultă din relația dintre angajator și angajat. Având în vedere dezechilibrul de puteri, angajații își pot da consimțământul liber numai în situații excepționale, atunci când nu există deloc consecințe legate de acceptarea sau respingerea unei oferte."

În acest sens, s-a subliniat că atunci când se solicită consimțământul, este necesar să se evalueze dacă această solicitare întrunește toate condițiile de obținere a unui consimțământ valabil. Per a contrario, consimțământul nu va fi un temei legal în ceea ce privește prelucrarea și, în consecință, aceasta nu va fi o prelucrare "în mod legal" așa cum prevede primul principiu din art. 5 al RGPD, fiind necesară identificarea unui alt temei legal din Regulament.

În ceea ce privește responsabilitatea operatorului, Autoritatea națională de supraveghere a precizat că art. 24 din RGPD 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."

Totodată, s-au menționat dispozițiile art. 32 din RGPD, potrivit cărora:

"Având în vedere stadiul actual al dezvoltării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul şi persoana împuternicită de acesta implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc".

Referitor la obligația de informare a persoanei vizate (angajatul, potențialul client), s-a subliniat că operatorii trebuie să ia măsuri adecvate pentru a furniza persoanei vizate informaţiile menţionate la articolele 13 sau 14 din RGPD, după caz, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu.

Prin urmare, față de cele prezentate în adresa transmisă, Autoritatea națională de supraveghere a considerat că prelucrarea datelor cu caracter special (orientarea sexuală, identitatea de gen, dizabilitatea și originea etnică) prin programul de diversitate și incluziune nu se poate realiza decât cu respectarea prevederilor legale din RGPD mai sus menționate.

► ***Prelucrarea datelor personale de către companiile care utilizează un serviciu de call-center***

O societate de avocatură a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la unele aspecte legate de prelucrarea datelor personale de către companiile care utilizează un serviciu de call-center (ex. pentru preluare a apelurilor clienților sau persoanelor interesate, răspund la întrebările acestora, inițiază apeluri cu utilizatori pentru furnizarea de informații/comunicări, uneori pe baza unor script-uri prestabilite).

Referitor la modalitatea de prelucrare a datelor cu caracter personal, inclusiv sub aspectul colectării, stocării, divulgării prin transmitere, diseminare sau punerea la dispoziție în orice alt mod, potrivit Regulamentului (UE) 2016/679, s-a precizat că aceasta se realizează cu consimțământul persoanei vizate sau în alte condiții legale în care nu se solicită consimțământul, prevăzute de art. 6, art. 9 sau art. 10, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

În ceea ce privește consimțământul persoanei vizate, Autoritatea națională de supraveghere a subliniat că art. 4 pct. 11 din Regulamentul (UE) 2016/679 precizează că acesta înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

Autoritatea națională de supraveghere a mai arătat faptul că în cadrul prelucrării datelor este necesară respectarea principiilor stabilite de art. 5 din RGPD, inclusiv principiul responsabilității, potrivit căruia operatorul este responsabil de respectarea acestor principii şi poate demonstra această respectare.

Ca atare, s-a precizat că fiecărui operator îi revine obligația de a analiza, în funcție de specificul tuturor activităților efectiv realizate, fiecare prelucrare de date personale efectuată, să decidă cu privire la legitimitatea prelucrării și, în același timp, să ia toate măsurile necesare pentru respectarea drepturilor persoanelor vizate, precum și pentru asigurarea securității și confidențialității datelor, raportat la prevederile legale menționate.

► ***Prelucrarea de date biometrice în vederea acordării de servicii financiare***

O societate de avocatură s-a adresat Autorității naționale de supraveghere și a solicitat o opinie cu privire la prelucrarea imaginii unei persoane fizice în cadrul unui proces de comparare, prin utilizarea unui soluții bazate pe biometrie facială a unei fotografii ("selfie") a acesteia cu imaginea sa din actul de identitate, în procesul de "cunoaștere a clientelei anterior inițierii unei relații de afaceri" de către o entitate care intră sub incidența prevederilor Legii nr. 129/2019 pentru prevenirea şi combaterea spălării banilor şi finanţării terorismului, precum şi pentru modificarea şi completarea unor acte normative, cu modificările și completările ulterioare.

În considerarea celor descrise în adresa transmisă, respectiv faptul că entitatea care intră sub incidența prevederilor Legii nr. 129/2019 intenționa să utilizeze un procedeu de identificarea electronică "la distanță" a clienților persoane fizice care ar fi dorit să acceseze serviciile entității, comparând imaginea persoanei din cartea de identitate cu o fotografie făcută de aceasta și transmisă entității, prin utilizarea unui "soft de biometrică facială", Autoritatea națională de supraveghere a precizat următoarele:

Art. 4 din Regulamentul (UE) 2016/679 stabilește o serie de definiții, printre care și pe cea a "datelor biometrice". Astfel, art. 4 pct. 14 din RGPD definește datele biometrice ca

fiind "date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice".

Corelat cu cele de mai sus, în documentul intitulat "Avizul 3/2012 privind progresele înregistrate de tehnologiile biometrice", Grupul de Lucru Art. 29 (în prezent, Comitetul European pentru Protecția Datelor) menționează că "există două categorii principale de tehnici biometrice", unele dintre acestea referindu-se la "tehnici bazate pe caracteristici fizice și fiziologice, care măsoară caracteristicile fizice și fiziologice ale unei persoane și care includ: verificarea amprentelor digitale, analiza imaginii degetului, recunoașterea irisului, analiza retinei, recunoașterea facială, modelul conturului mâinii, recunoașterea formei urechilor, detectarea mirosului corporal, recunoașterea vocală, analiza tiparului ADN, analiza porilor sudoripari etc."

Referitor la prelucrarea datelor biometrice (imaginea facială), aceasta este supusă condițiilor art. 9 din RGPD, coroborate cu art. 3 din Legea nr. 190/2018. În acest context, Autoritatea națională de supraveghere a subliniat faptul că dispozițiile art. 3 alin. (1) din Legea nr. 190/2018 devin aplicabile în situația prelucrării datelor biometrice în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri. În caz contrar, se aplică dispozițiile art. 9 din RGPD.

Astfel, conform art. 9 alin. (2) lit. a) din RGPD, datele biometrice pot fi prelucrate dacă persoana vizată şi-a dat consimţământul explicit pentru prelucrarea acestor date pentru unul sau mai multe scopuri specifice.

Totodată, art. 22 din RGPD prevede următoarele:

"(1) Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

(2) Alineatul (1) nu se aplică în cazul în care decizia:

a) este necesară pentru încheierea sau executarea unui contract între persoana vizată şi un operator de date;

b) este autorizată prin dreptul Uniunii sau dreptul intern care se aplică operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate; sau

c) are la bază consimţământul explicit al persoanei vizate.

(3) În cazurile menţionate la alineatul (2) literele (a) şi (c), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate, cel puţin dreptul acesteia de a obţine intervenţie umană din partea operatorului, de a-şi exprima punctul de vedere şi de a contesta decizia.

(4) Deciziile menţionate la alineatul (2) nu au la bază categoriile speciale de date cu caracter personal menţionate la articolul 9 alineatul (1), cu excepţia cazului în care se aplică articolul 9 alineatul (2) litera (a) sau (g) şi în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale persoanei vizate."

În ceea ce privește consimțământul persoanei vizate, art. 4 pct. 11 din RGPD precizează că acesta înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

Considerentul (32) din RGPD prevede următoarele: "Consimţământul ar trebui acordat printr-o acţiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoştinţă de cauză şi clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declaraţie făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuţe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societăţii informaţionale sau orice altă declaraţie sau acţiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absenţa unui răspuns, căsuţele bifate în prealabil sau absenţa unei acţiuni nu ar trebui să constituie un consimţământ. Consimţământul ar trebui să vizeze toate activităţile de prelucrare efectuate în acelaşi scop sau în aceleaşi scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimţământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimţământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară şi concisă şi să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimţământul."

Considerentul (42) din RGPD precizează: "În cazul în care prelucrarea se bazează pe consimţământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată şi-a dat consimţământul pentru operaţiunea de prelucrare. În special, în contextul unei declaraţii scrise cu privire la un alt aspect, garanţiile ar trebui să asigure că

persoana vizată este conştientă de faptul că şi-a dat consimţământul şi în ce măsură a făcut acest lucru. În conformitate cu Directiva 93/13/CEE a Consiliului (sbl. ns. Directiva privind clauzele abuzive în contractele încheiate cu consumatorii), ar trebui furnizată o declaraţie de consimţământ formulată în prealabil de către operator, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, iar această declaraţie nu ar trebui să conţină clauze abuzive. Pentru ca acordarea consimţământului să fie în cunoştinţă de cauză, persoana vizată ar trebui să fie la curent cel puţin cu identitatea operatorului şi cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimţământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să îşi retragă consimţământul fără a fi prejudiciată."

În același timp, s-a precizat faptul că în documentul intitulat "Orientări asupra Consimțământului în temeiul Regulamentului 2016/679" (WP 259/Versiunea 1.1 adoptată în 4 mai 2020), fostul Grup de Lucru Art. 29 (în prezent Comitetul european pentru protecția datelor) menționa următoarele:

"În general, consimțământul poate fi temeiul juridic adecvat doar atunci când persoanei vizate i s-a acordat controlul și posibilitatea unei alegeri reale în ceea ce privește fie acceptarea fie respingerea termenilor conferiți sau respingerea acestora fără nici un prejudiciu. Atunci când se solicită consimțământul, un operator de date are obligația să evalueze dacă această solicitare întrunește toate condițiile de obținere a unui consimțământ valabil. Dacă este obținut în conformitate deplină cu GDPR, consimțământul este un instrument care conferă persoanelor vizate controlul asupra posibilității ca datele lor cu caracter personal să fie sau nu prelucrate. Altfel, controlul deținut de persoanele vizate devine iluzoriu și consimțământul va fi un temei anulabil în ceea ce privește prelucrarea, cu consecința că activitatea de prelucrare este nelegală".

Același document menționează: "Dacă un operator poate demonstra că un serviciu include posibilitatea de retragere a consimțământului fără consecințe negative, (...) acest lucru poate servi la demonstrarea faptului că consimțământul a fost exprimat în mod liber. RGPD nu exclude toate stimulentele, dar îi revine operatorului sarcina să demonstreze că consimțământul a fost exprimat în continuare în mod liber în toate circumstanțele."

În contextul celor de mai sus, în procedeul descris în adresa transmisă Autorității nu s-au identificat precizările necesare cu privire la respectarea tuturor dispozițiilor din RGPD

menționate, ținând cont de natura datelor prelucrate (inclusiv din categoria celor speciale) și modalitatea de obținere a acestora. Autoritatea națională de supraveghere a precizat că este necesar ca operatorul să se asigure de faptul că persoanele vizate vor fi informate potrivit art. 13 din RGPD, astfel încât să fie respectat principiul transparenței.

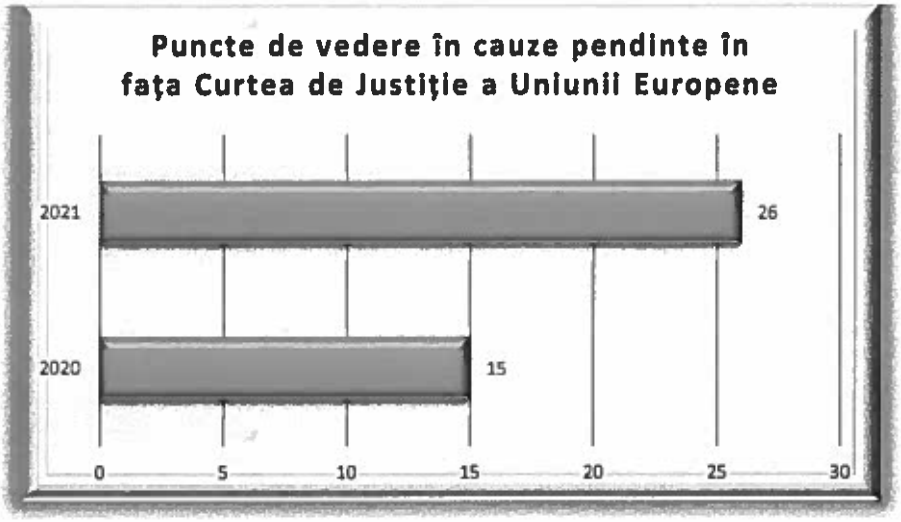
În acest context, Autoritatea națională de supraveghere a subliniat faptul că potrivit principiului responsabilității (art. 24 RGPD), operatorul trebuie să demonstreze că prelucrarea se efectuează în conformitate cu RGPD, iar atunci când măsurile luate sunt proporţionale în raport cu operaţiunile de prelucrare, acestea includ punerea în aplicare de către operator a unor politici adecvate de protecţie a datelor.

De asemenea, operatorul trebuie să asigure, în conformitate cu art. 25 din RGPD, protecţia datelor începând cu momentul conceperii şi în mod implicit (principiile privacy by design și privacy by default).

Așadar, s-a subliniat faptul că este necesar a se avea în vedere cerințele legale prezentate anterior, în vederea asigurării conformității prelucrării datelor, inclusiv sub aspectul obligațiilor stabilite prin același Regulament și al necesității asigurării unei protecţii eficiente a drepturilor persoanelor vizate.

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

În anul 2021 au fost transmise puncte de vedere ale Autorității naționale de supraveghere către Ministerul Afacerilor Externe, în **26 cauze** pendinte în fața Curții de Justiție a Uniunii Europene, număr mai mare față de cel din anul 2020.



Cauzele analizate au avut ca obiect interpretarea anumitor articole din acte normative comunitare (Regulamentul (UE) 2016/679, Directiva 95/46/CE, Directiva 2002/58/CE, precum și din alte acte comunitare ce conțin prevederi cu implicații în ceea ce privește prelucrarea datelor cu caracter personal), astfel:

► **Cauza C-154/21** în cadrul căreia cererea a fost adresată de o instanță din Austria (Oberster Gerichtshof) cu privire la interpretarea **art. 15 alin. (1) lit. c) din Regulamentul (UE) 2016/679.**

► **Cauza C-252/21** în cadrul căreia cererea a fost adresată de o instanță din Germania cu privire la interpretarea dispozițiilor **art. 51 și următoarele din Regulamentul (UE) 2016/679 și ale art. 4 alin. (3) TFUE.**

► **Cauza C-548/21** în cadrul căreia cererea a fost adresată de o instanță din Austria (Landesverwaltungsgericht Tirol) cu privire la interpretarea **art. 15 alin. (1) din Directiva 2002/58.**

► **Cauza C-560/21** în cadrul căreia cererea a fost adresată de o instanță din Germania (Bundesarbeitsgericht) cu privire la interpretarea **art. 38 alin. (3) a doua teză din Regulamentul (UE) 2016/679.**

► **Cauza C-45/21 Banka Slovenjke** în cadrul căreia cererea a fost adresată de o instanță de trimitere din Slovenia (Ustavno sodišče Republike Slovenije), referitoare la analizarea situației "Procedură de control al constituționalității; obligație de despăgubire în sarcina unei bănci centrale naționale față de foștii titulari ai unor instrumente financiare anulate, pe care aceasta a decis să le anuleze în exercitarea competenței sale conferite de

lege de a adopta măsuri cu caracter extraordinar în interes public în scopul prevenirii amenințărilor la adresa stabilității sistemului financiar; principiul independenței financiare a băncii centrale naționale; confidențialitatea informațiilor confidențiale primite sau constituite în cadrul supravegherii prudențiale a băncilor".

► **Cauza C-77/21, Digi Távközlési és Szolgáltató Kft.** în cadrul căreia cererea a fost adresată de o instanță de trimitere din Ungaria (Fővárosi Törvényszék), în ceea ce privește interpretarea cerințelor **art. 5 alin. (1) lit. b) și e) din Regulamentul (UE) 2016/679**, inclusiv referitor la interpretarea noțiunii de „limitări legate de scop".

► **Cauza C-334/21 Procura Della Republica di Rieti** în cadrul căreia cererea a fost adresată de o instanță de trimitere din Italia. Procedura a fost suspendată până la pronunțarea hotărârii în Cauza C-140/20. Ulterior cererea preliminară a fost retrasă de către instanța de trimitere din Italia.

► **Cauza C-349/21** în cadrul căreia cererea a fost adresată de o instanță de trimitere din Bulgaria referitoare la interpretarea dispozițiilor **art. 15 alin. (1)**, coroborat cu **art. 5 alin. (1) din Directiva 2002/58** privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și cu **considerentul (11)** al acesteia, în contextul practicii unor instanțe din Bulgaria în cadrul procedurilor penale, în mod special referitor la modalitatea de redactare a deciziei judecătorești de autorizare a prelucrării datelor cu caracter personal în scopuri probatorii.

► **Cauza C-350/21** în cadrul căreia cererea a fost adresată de o instanță de trimitere din Bulgaria, întrebările preliminare fiind legate de interpretarea dispozițiilor **art. 15 alin. (1), coroborat cu art. 5 alin. (1) și cu considerentul (11) din Directiva 2002/58**, în contextul procedurii pe care trebuie să o urmeze organele de urmărire penală din Bulgaria în fața instanțelor naționale, având în vedere conținutul deciziei judecătorești de autorizare a prelucrării datelor cu caracter personal în scopuri probatorii, raportat la legislația națională din Bulgaria.

► **Cauza C-446/21** în cadrul căreia cererea a fost adresată de o instanță din Austria, referitoare la interpretarea dispozițiilor **art. 5 alin. (1) lit. b) și c), art. 6 alin. (1) lit. a) și b) și art. 9 din Regulamentul (UE) 2016/679.**

► **Cauza C-487/21** în cadrul căreia cererea a fost adresată de o instanță din Austria, referitoare la interpretarea dispozițiilor **art. 15 alin. (3) din Regulamentul (UE) 2016/679.**

► **Cauza C-552/21** în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea **art. 77 alin. (1), art. 17 și art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679.**

► **Cauza C-34/21** în cadrul căreia cererea a fost adresată de o instanță din Germania (Landul Heseen), referitoare la interpretarea **art. 88 din Regulamentul (UE) 2016/679.**

În această cauză, Autoritatea națională de supraveghere a apreciat ca fiind oportună înaintarea de observații scrise de către Guvernul României, având în vedere în ceea ce privește art. 88 alin. (1) din Regulamentul (UE) 2016/679, că acesta trebuie interpretat în sensul că, pentru a fi o normă mai detaliată care urmărește să asigure protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, așa cum prevede art. 88 alin. (1) din RGPD, o normă de drept intern trebuie să îndeplinească cel puțin cerințele impuse de dispoziții precum cele prevăzute la art. 88 alin. (2) din RGPD, având în vedere și prevederile art. 6 alin. (2) și (3) din același regulament.

► **Cauza C-129/21** în cadrul căreia cererea a fost adresată de o instanță din Belgia, raportat la întrebările adresate Curții referitoare la interpretarea **art. 5, art. 17 și art. 24 din Regulamentul (UE) 2016/679**, precum și a **art. 12 din Directiva 2002/58** coroborat cu **art. 2** din aceeași directivă și cu **art. 95 din RGPD**.

În această cauză, Autoritatea națională de supraveghere a apreciat ca fiind oportună înaintarea de observații scrise de către Guvernul României având în vedere faptul că aspectele puse în discuție vizează relația Regulamentului (UE) 2016/679 cu Directiva 2002/58/CE, respectiv dreptul de ștergere garantat de regulament și „consimțământul" abonatului în sensul RGPD ca temei pentru publicarea datelor abonatului în liste de abonați și servicii de informații telefonice accesibile publicului, oferite de operatorul însuși sau de furnizori terți.

► **Cauza C-132/21** în cadrul căreia cererea a fost adresată de o instanță din Ungaria, referitoare la interpretarea **art. 77 alin. (1) și art. 79 alin. (1) din Regulamentul (UE) 2016/679.**

► **Cauza C-180/21** în cadrul căreia cererea a fost adresată de o instanță din Bulgaria, referitoare la interpretarea dispozițiilor **art. 1 alin. (1) din Directiva 2016/680** și ale **Regulamentului 2016/679** raportat la **art. 3 pct. 8 din directivă, precum și ale art. 6 alin. (1) lit. f) din Regulamentul (UE) 2016/679.**

► **Cauza C-268/21** în cadrul căreia cererea a fost adresată de o instanță din Suedia, referitoare la interpretarea dispozițiilor **art. 6 alin. (3) și (4) din Regulamentul (UE) 2016/679.**

► **Cauza C-300/21** în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor **art. 85 din Regulamentul (UE) 2016/679**.

► **Cauza C-340/21** în cadrul căreia cererea a fost adresată de o instanță din Bulgaria, referitoare la interpretarea dispozițiilor **art. 24, art. 32 și art. 82 alin. (1), (2) și (3) din Regulamentul (UE) 2016/679.**

► **Cauza C-579/21** în cadrul căreia cererea a fost adresată de o instanță din Suedia, referitoare la interpretarea dispozițiilor **art. 15 alin. (1) din Regulamentul (UE) 2016/679**.

► **Cauza C-634/21** în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor **art. 22 din Regulamentul (UE) 2016/679**.

► **Cauza C-667/21** în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor **art. 9 alin. (2) lit. h)** și **art. 82 alin. (1) din Regulamentul (UE) 2016/679.**

► **Cauza C-687/21** în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor **art. 82 din Regulamentul (UE) 2016/679**.

► **Cauza C-205/21** în cadrul căreia cererea a fost adresată de o instanță din Bulgaria, referitoare la interpretarea dispozițiilor **art. 4 alin. (1) lit. a - c, art. 6 lit. (a), art. 8 alin. (1) și (2), art. 10 din Directiva 2016/680** raportat la **Legea privind Ministerul de Interne din Bulgaria**, coroborat cu **art. 9 din Regulamentul (UE) 2016/679, respectiv art. 3, art. 8 și art. 48 din Cartă.**

► **Cauza C-453 (X-FAB Dresden GmbH&Co.KG)** în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea dispozițiilor **art. 38 alin. (3) teza a II-a din Regulamentul (UE) 2016/679, prin raportare la art. 37 alin. (1) Regulamentul (UE) 2016/679 și art. 267 TFUE.**

► **Cauza C-470** (La Quadrature du Net e.a.) în cadrul căreia cererea a fost adresată de o instanță din Franța, referitoare la interpretarea dispozițiilor **art. 15** din Directiva asupra

confidențialității și comunicațiilor electronice, articolelor **7, 8, 11 și 52 din Carta drepturilor fundamentale a Uniunii Europene** și **Regulamentului (UE) 2016/679**.

■ Puncte de vedere exprimate în contextul analizării codurilor de conduită

O asociație non-profit din România a transmis un Cod de conduită pentru eventuale recomandări privind corectarea sau completarea prevederilor acestuia în acord cu dispozițiile Regulamentului (UE) 2016/679.

Faţă de conținutul Codului, s-a recomandat reanalizarea proiectul transmis astfel încât să prevadă măsuri și soluții particularizate activității din domeniul marketingului direct și publicității on-line pentru a se asigura respectarea Regulamentului General privind Protecția Datelor în sectorul de activitate vizat. Cât privește tipurile de date cu caracter personal prelucrate, s-a recomandat reanalizarea datelor care pot fi prelucrate în scopurile declarate prin raportare la principiul proporționalității, statuat de art. 5 din RGPD.

În ceea ce privește rolurile părților implicate în furnizarea serviciilor de publicitate on-line, s-a recomandat clarificarea aspectelor legate de atribuțiile părților implicate în furnizarea de servicii on-line prin raportare la defințiile stabilite de art. 4 din RGPD, obligațiile operatorului/împuternicitului prevăzute la Secțiunea IV din Regulament "Operatorul și persoana împuternicită de operator", ținând cont totodată și de celelalte principii de prelucrare prevăzute de art. 5 din RGPD.

Autoritatea națională de supraveghere a solicitat clarificarea mențiunilor din Codul de conduită analizat referitoare la temeiul prelucrării, mai ales în contextul în care titlurile secțiunilor codului se referă la consimțământ însă, la parcurgerea acestora, s-a observat că se fac trimiteri, intermitent, la consimțământ sau la informare, aspect ce ar putea crea confuzie la încheierea contractelor.

De asemenea, s-a precizat cu privire la Codul de conduită supus atenției Autorității, faptul că este necesar ca acesta să fie redactat într-o manieră accesibilă tuturor operatorilor/împuterniciților cărora li se adresează, "pentru a se asigura prelucrarea datelor cu caracter personal ale utilizatorilor de internet în condiții de interpretare adecvată și unitară la nivelul industriei de profil".

Autoritatea națională de supraveghere a recomandat să se aibă în vedere și Ghidul nr. 1/2019 privind codurile de conduită și organismele de monitorizare a acestor coduri, emis de Comitetul European privind Protecția Datelor.

▪ Activitatea de analiză și soluționare a plângerilor prealabile

Potrivit art. 21 alin. (6) din Legea nr. 102/2005, republicată, în măsura în care persoana vizată este nemulțumită de răspunsul primit ca urmare a depunerii plângerii sale la Autoritatea națională de supraveghere, aceasta se poate adresa secției de contencios administrativ a tribunalului competent, după parcurgerea procedurii prealabile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare.

Astfel, pe parcursul anului 2021 au fost depuse la Autoritatea națională de supraveghere un număr de **15 plângeri prealabile.**

Dintre plângerile prealabile formulate în condițiile legii, urmare a reanalizării susținerilor și dovezilor transmise de către petenți, **au fost admise 8**, raportat la aspectele semnalate de către persoanele vizate în cauză.

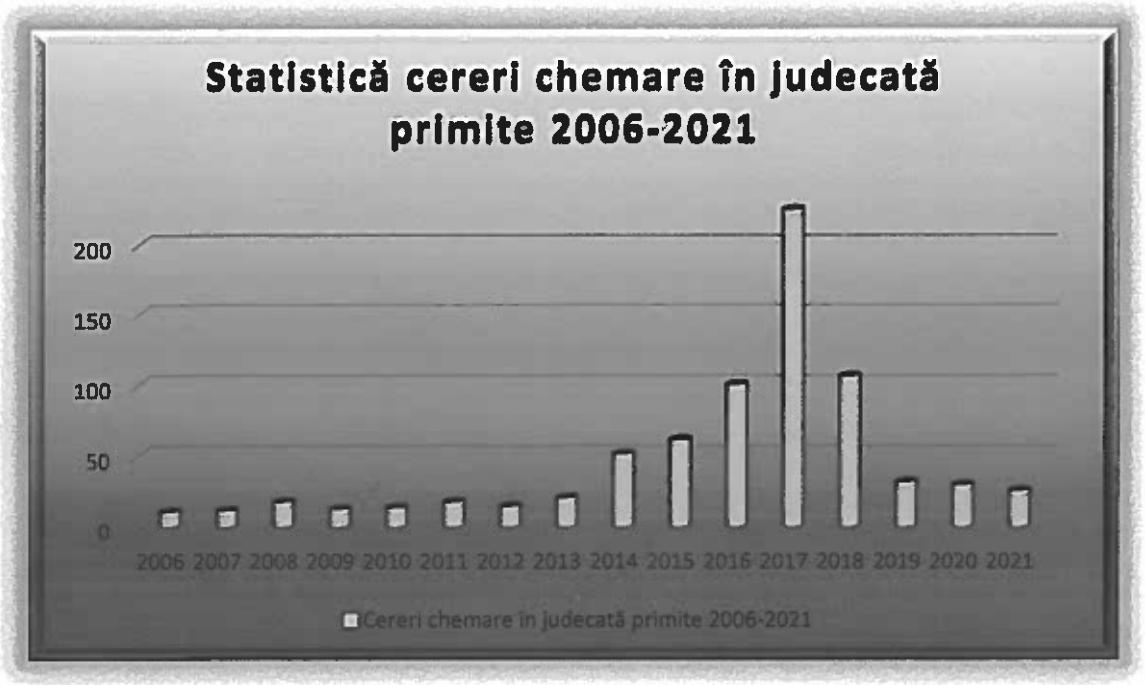
Secțiunea a 4 – a

Activitatea de reprezentare în fața instanțelor de judecată

În anul 2021, Autoritatea națională de supraveghere a gestionat un număr de **152 dosare** aflate pe rolul instanțelor de judecată în diferite stadii procesuale.

Dintre acestea, pe parcursul anului 2021 au fost înregistrate pe rolul instanțelor de judecată un număr de **25 de cereri noi de chemare în judecată** întemeiate pe Regulamentul (UE) 2016/679, pe Legea nr. 506/2004 sau pe Legea nr. 554/2004 a contenciosului administrativ.

Menționăm că **6 cereri de chemare în judecată** au avut ca obiect contestarea proceselor–verbale de constatare/sancționare încheiate de Autoritatea națională de supraveghere.



În anul 2021 au fost finalizate mai multe acțiuni în mod favorabil pentru instituția noastră, atât sub incidența legislației anterioare privind protecția datelor (Legea nr. 677/2001), cât și sub incidența Regulamentului (UE) 2016/679, dintre care prezentăm mai jos câteva **cazuri relevante:**

1. Hotărâre definitivă pronunțată într-un litigiu privind încălcarea art. 5 alin. (1) lit. d) și f), art. 5 alin. (2), art. 25, art. 32 și art. 33 alin. (1) din RGPD.

Autoritatea națională de supraveghere a efectuat o investigație, în anul 2019, ca urmare a unei plângeri a unui petent prin care acesta sesiza încălcări ale prelucrării datelor de către un operator din domeniul financiar-nebancar, prin transmiterea pe adresa sa de e-mail a unor documente ce conțineau datele personale ale unei alte persoane. În urma acestei investigații s-a constatat că operatorul a prelucrat datele fără să dovedească aplicarea unor mecanisme eficiente de verificare și validare a exactității datelor colectate și ulterior prelucrate, respectiv de păstrare a confidențialității acestora, conform principiilor prevăzute la art. 5 din RGPD.

De asemenea, s-a constatat că operatorul nu a luat suficiente măsuri de securitate a datelor personale, potrivit art. 25 și art. 32 din RGPD, astfel încât să evite dezvăluirea neautorizată și accesibilă a datelor personale către terți. Totodată, operatorul nu a notificat Autorității naționale de supraveghere incidentul de securitate ce i-a fost adus la cunoștință, potrivit art. 33 din RGPD, în termen de 72 de ore de la data la care a luat cunoștință de acesta.

Prin urmare, operatorul a fost sancționat contravențional cu mai multe amenzi în cuantum total de 66.901,8 lei (echivalentul a 14.000 EUR)

În același timp, operatorului i s-au aplicat și următoarele măsuri corective:

- măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de colectare și prelucrare ulterioară a datelor personale în scopul încheierii și executării contractelor de împrumut, în special, sub aspectul verificării datelor personale colectate, precum adresa de poștă electronică, ce permit comunicarea la distanță a datelor personale, prin implementarea unor metode eficiente de validare a exactității datelor - în termen de 30 zile de la data comunicării procesului-verbal de contravenție (art. 58 alin. (2) lit. d) din RGPD);

- măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de prelucrare a datelor personale în scopul încheierii și executării contractelor de împrumut, în vederea respectării secretului profesional și a confidențialității datelor personale ale clienților săi, în special, în cazul transmiterii unor documente și mesaje ce conțin date personale la distanță (de exemplu, prin poșta electronică), prin implementarea unor măsuri adecvate și eficiente de securitate, atât din punct de vedere tehnic (precum criptarea), cât și din punct de vedere organizatoric, prin instruirea persoanelor ce prelucrează date sub autoritatea sa, în vederea identificării și limitării imediate a riscurilor ce pot afecta persoanele vizate - în termen de 30 zile de la data comunicării procesului-verbal de contravenție (art. 58 alin. (2) lit. d) din RGPD);

- măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de prelucrare a datelor personale în scopul implementării unei politici interne adecvate pentru identificarea riscurilor, analiza acestora și notificarea către Autoritatea națională de supraveghere în cazul producerii unei încălcări a securității, în condițiile prevăzute de art. 33 alin. (1) din RGPD - în termen de 30 zile de la data comunicării procesului-verbal de contravenție (art. 58 alin. (2) lit. d) din RGPD).

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

Analizând probatoriul administrat în cauză, Tribunalul București, Secția a II-a Contencios Administrativ și Fiscal, a admis în parte cererea de chemare în judecată formulată de operator și a dispus înlocuirea sancțiunii amenzii cu aceea a avertismentului.

Cu privire la temeinicia procesului-verbal de contravenție, *instanța a apreciat* că *„procesul verbal a fost încheiat cu respectarea dispozițiilor legale"* și a reținut *„existența faptei cu conținut contravențional și vinovăția petentei la săvârșirea acesteia".*

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

Curtea de Apel București a admis apelul formulat de Autoritatea națională de supraveghere și a schimbat în parte sentința apelată, în sensul că a respins în tot cererea de chemare în judecată formulată de operat, ca nefondată.

Cu privire la vinovăție Curtea de Apel București a apreciat că *„reclamanta a fost sancționată pentru un cumul de abateri, pentru niciuna dintre acestea, raportat la gradul de pericol social ridicat, neimpunându-se aplicarea sancțiunii avertismentului, cu atât mai puțin sancțiunea finală putând fi cea a „avertismentului", astfel cum eronat a apreciat instanța de fond"*.

De asemenea, instanța a apreciat că *„faptele reținute în sarcina acesteia prezintă un grad de pericol social ridicat, astfel că amenda finală aplicată se impune a fi menținută."*

Pe cale de consecință, Curtea de Apel a confirmat corectitudinea procesului-verbal încheiat și a amenzii aplicate de instituția noastră.

Hotărârea judecătorească favorabilă Autorității naționale de supraveghere a rămas definitivă.

2. Hotărâre definitivă pronunțată într-un litigiu privind încălcarea securității prelucrării

Autoritatea națională de supraveghere a fost notificată în anul 2019 cu privire la producerea unei încălcări a securității datelor cu caracter personal la nivelul unei instituții financiar-bancare, conform prevederilor art. 33 din Regulamentul (UE) 2016/679.

Conform notificării transmise a reieșit faptul că două angajate ale operatorului instituție financiar-bancară, utilizând datele din documentele de identitate ale unor persoane fizice, transmise de către angajați ai unei alte societăți, instituție financiar nebancară, prin intermediul aplicației mobile WhatsApp, au efectuat interogări în sistemul Biroului de Credit SA, pentru a obține datele necesare în vederea determinării eligibilității la creditare a respectivelor persoane fizice vizate, printr-o simulare de prescoring (1194 simulări de prescoring, cu privire la 1177 persoane fizice). De asemenea, pentru 124 de persoane fizice vizate s-a efectuat și consultarea bazei de date a Agenției Naționale de Administrare Fiscală.

Simulările de prescoring menționate mai sus au fost efectuate prin intermediul aplicației informatice utilizate de instituția financiar-bancară (bancă) în activitatea de creditare, cu încălcarea procedurilor interne. În urma simulărilor de prescoring menționate, decizia negativă de creditare a fost comunicată de angajatele băncii către angajații instituției financiare nebancare.

În acest context, Autoritatea națională de supraveghere a efectuat investigații la cele două entități.

În urma investigației derulate la operatorul instituție financiară-nebancară s-a încheiat un proces-verbal de constatare/sancționare prin care au fost aplicate două sancțiuni cu amendă în cuantum total de 95.024 lei (echivalentul a 20.000 euro) pentru:

- încălcarea art. 32 alin. (4) coroborat cu art. 32 alin. (1) și alin. (2) din RGPD, în temeiul art. 58 alin. (2) lit. i) din RGPD, raportat la art. 14 alin. (11) și art. 15 alin. (1) și alin. (6) din Legea nr. 102/2005, republicată, precum și la art. 12 din Legea nr. 190/2018 coroborat cu art. 8 din Ordonanța Guvernului nr. 2/2001 și

- încălcarea art. 33 alin. (1) din RGPD, în temeiul art. 58 alin. (2) lit. i) din RGPD, raportat la art. 14 alin. (11) și art. 15 alin. (1) și alin. (6) din Legea nr. 102/2005, republicată, precum și la art. 12 din Legea nr. 190/2018, coroborat cu art. 8 din Ordonanța Guvernului nr. 2/2001.

Procesul-verbal de constatare/sancționare a fost contestat de instituția financiară nebancară sancționată, iar instanța de fond – Tribunalul Ilfov, în mod corect a reținut că: *"(...) reclamantul a fost sancționat pentru nerespectarea prevederilor art. 32 alin. 4 coroborat cu art. 32 alin. 1 și 2 din Regulament conform cărora operatorul și persoana împuternicită de acesta iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub*

autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la datele cu caracter personal nu le prelucrează decât la cererea operatorului, cu excepția cazului în care această obligație îi revine în temeiul dreptului uniunii sau a dreptului intern."

În același timp, în mod corect *"Instanța reține că reclamantul prin cererea formulată nu a negat fapta săvârșită de către angajații săi, operațiunile de prelucrare a datelor fiind efectuate în exercitarea atribuțiilor de serviciu.*

Conform art. 32 alin. 1 din Regulament operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitatate corespunzător acestui.

Așadar, reclamantul avea obligația de a implementa măsuri efective pentru a asigura un nivel de securitate corespunzător, simpla elaborare de acte ca cele enumerate în cerere nefiind suficientă având în vedere că prin acest mecanism se urmărește protejarea datelor cu caracter personal al cetățenilor, respectiv dreptul la viață privată."

De altfel, similar cu Autoritatea națională de supraveghere, în mod corect instanța de fond a reținut:

"Referitor la cea de-a doua contravenție reținută în sarcina reclamantului instanța reține că potrivit art. 33 alin. 1 din Regulament în cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru Autorității de supraveghere competente, în temeiul art. 55, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice."

"(...) reclamanta nu a făcut dovada că a informat clienții cu privire la operațiunile de prelucrare, ori în lipsa exprimării unui consimțământ în scris, Regulamentul prevede că acceptarea trebuie să fie fără echivoc.

Concluzionând, reținând că potrivit art. 7 din Regulament operatorul trebuie să facă dovada existenței consimțământului instanța reține că în mod corect s-a reținut în sarcina sa incidența prevederilor art. 33 alin. 1 din Regulament."

De asemenea, instanța de fond a mai reținut că: *"Raportat la gravitatatea faptei reținută în sarcina sa, instanța apreciază că amenda aplicată este proporțională, având în vedere că reclamantul avea obligația de a asigura protecția datelor cu caracter personal care constituie un drept fundamental, art. 8 alin. (1) din CDFUE și art. 16 alin. (1) din TFUE*

reglementând dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc."

Hotărârea instanței de fond, favorabilă Autorității naționale de supraveghere, a rămas definitivă prin respingerea apelului formulat de instituția financiară nebancară sancționată.

Secțiunea a 5-a:
Informare publică

Autoritatea națională de supraveghere a continuat, în anul 2021, **activitățile de comunicare** destinate informării publicului larg, cu privire la regulile de prelucrare a datelor cu caracter personal, în contextul Regulamentului (UE) 2016/679, raportat la contextul pandemic specific acestui an, în mod predominant on-line.

Astfel, prezentăm succint cele mai relevante dintre aceste manifestări:

♦ **Ziua Europeană a Protecției Datelor – 28 Ianuarie 2021**

Ziua Europeană a Protecției Datelor a fost sărbătorită în data de 28 ianuarie 2021 de către toate statele membre ale Consiliului Europei și a marcat 40 de ani de la adoptarea, în anul 1981, la Strasbourg, a Convenției 108 pentru protecția persoanelor referitoare la prelucrarea automatizată a datelor cu caracter personal.

Pentru celebrarea Zilei Europene a Protecției Datelor, Autoritatea națională de supraveghere a organizat **două evenimente on-line** destinate informării corecte a operatorilor cu privire la aplicarea adecvată a regulilor de protecție a datelor personale, statuate de Regulamentul General privind Protecția Datelor.

Astfel, **pe data de 27 ianuarie 2021, a fost organizată on-line, o conferință dedicată autorităților și instituțiilor publice**, intitulată „Constatări și recomandări pentru operatorii din sectorul public", în care au fost prezentate aspecte practice specifice de aplicare a principiilor de prelucrare a datelor personale.

Apoi, pe data de 28 ianuarie 2021, a fost organizată, on-line, **cea de-a doua conferință** dedicată marcării Zilei Europene a Protecției Datelor, cu tema „Constatări și

recomandări **pentru operatorii din sectorul privat**", cu participarea celor mai importante asociații și uniuni profesionale, a unor camere de comerț și a reprezentanților mass-media.

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 sintetice privind activitatea din anul anterior.

Totodată, 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.

♦ **Eveniment aniversar - trei ani de la aplicarea Regulamentului (UE) 2016/679– 25 Mai 2021**

Cu prilejul sărbătoririi a trei ani de la aplicarea Regulamentului (UE) 2016/679, Autoritatea naţională de supraveghere a organizat, în luna mai 2021, un **concurs on-line de eseuri** adresat studenților, având ca temă „Asigurarea protecției datelor în domeniul educațional în contextul pandemiei COVID-19".

De asemenea, pentru marcarea acestui eveniment, Autoritatea națională de supraveghere a postat pe site-ul instituției un comunicat de presă.

În același timp, instituția noastră a postat pe site-ul propriu și videoclipul pregătit la nivelul Comitetului european pentru protecția datelor.

♦ **Conferințe, simpozioane, seminarii, reuniuni**

Instituţia noastră a participat activ și în anul 2021 la **reuniuni** cu incidență în domeniul protecției datelor, organizate de diverse instituții publice sau de entități private, **în special în format on-line.**

În cadrul acestor evenimente, reprezentanții Autorității naționale de supraveghere au clarificat anumite aspecte privind condițiile utilizării datelor, respectarea drepturilor persoanelor vizate, asigurarea confidenţialităţii prelucrărilor de date cu caracter personal şi transferul datelor cu caracter personal către țări din afara Uniunii Europene, ceea ce reflectă continuitatea deschiderii către societatea civilă.

În acest context, menționăm că Autoritatea națională de supraveghere a participat la o serie de **reuniuni, simpozioane și seminarii, inclusiv on-line**, cum ar fi:

- conferința "Digitalizarea incluzivă", organizată de Secretariatul General al Guvernului;
- conferința "GDPR față în față cu realitatea", organizată de Asociația consilierilor juridici din sistemul financiar-bancar;
- reuniunea on-line cu MAE-MJ-MAI privind gestionarea externă a dosarului privind retenția datelor;
- reuniunea privind aplicarea Regulamentului (UE) 2021/953 privind cadrul pentru eliberarea, verificarea şi acceptarea certificatelor interoperabile de vaccinare, testare şi vindecare de COVID-19 (certificatul digital al UE privind COVID) pentru a facilita libera circulaţie pe durata pandemiei de COVID-19, organizată de Secretariatul General al Guvernului;
- reuniunea privind anumite acte normative organizată de Inspectoratul General al Poliției de Frontieră;
- dezbaterea on-line "Ce e special cu privire la datele personale?", organizată de juridice.ro;
- două webinarii on-line organizate de Asociația Specialiștilor în Confidențialitate și Protecția Datelor (ASCPD) în data 25 mai 2021, respectiv cele cu tema "Prelucrarea datelor în domeniul sanitar" și "Utilizarea consimțământului ca temei legal"; cele șase evenimente ce au marcat "Ziua responsabilului cu protecția datelor cu caracter personal", au fost destinate atât operatorilor de date personale cât și specialiștilor din domeniu și au abordat teme precum prelucrarea datelor în domeniul sanitar, prelucrarea datelor în învățământ, prelucrarea datelor în administrația publică, utilizarea consimțământului ca temei legal, măsurile tehnice și organizatorice și activitatea on-line a operatorilor;
- videoconferința solicitată de Asociația Română a Băncilor și Biroul de Credit SA pentru discutarea aspectelor referitoare la proiectul ARB și BC ce vizează "Identitatea financiară digitală";
- reuniunea de pregătire profesională în domeniul protecției datelor personale pentru personalul din cadrul Instituției Avocatul Poporului.

Pe de altă parte, subliniem că **personalul instituției noastre a acordat consiliere telefonică** unui număr semnificativ de operatori din mediul public și privat, precum și persoanelor fizice, 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, în condițiile în care activitatea de acordare a audiențelor la sediu s-a impus să fie suspendată în contextul evoluției pandemice și a stării de alertă.

În același timp, menționăm că Autoritatea națională de supraveghere a participat la reuniunile unor **grupuri de lucru interinstituționale** în vederea discutării pe marginea unor proiecte de acte normative pe care le-au inițiat unele ministere, dar și pe diverse chestiuni complexe ce țin de protecția datelor personale.

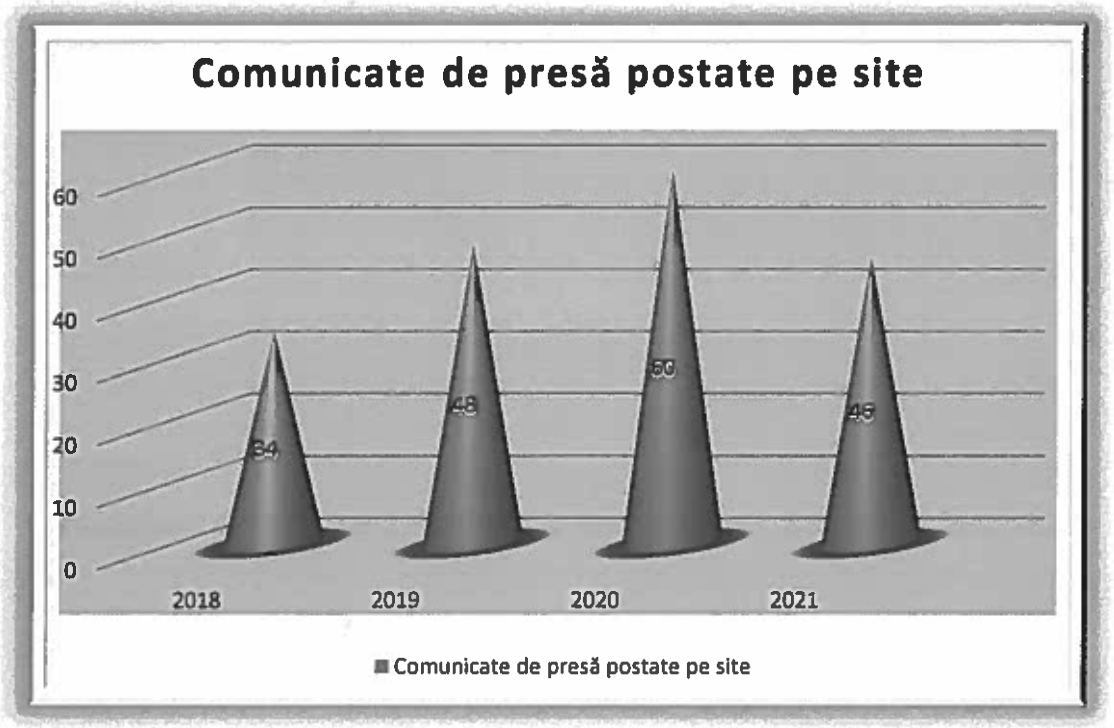
Totodată, Autoritatea națională de supraveghere a luat parte la **întâlniri** cu **autorități și instituții publice, inclusiv on-line**, precum: Oficiul Român pentru Drepturile de Autor (ORDA), Agenția Națională de Administrare Fiscală, Ministerul Educației și Cercetării, Ministerul Sănătății, Ministerul Afacerilor Interne, Ministerul Economiei, Antreprenoriatului și Turismului, Autoritatea pentru Digitalizarea României.

Reprezentanții instituției noastre au participat și la lucrări din **comisiile parlamentare de specialitate, inclusiv on-line,** în vederea susținerii unor propuneri sau proiecte de legi ce vizau aspecte de protecția datelor personale.

În ceea ce privește operatorii din sectorul privat, în cadrul unor videoconferințe dar și întâlniri de lucru la sediul Autorității naționale de supraveghere, au fost purtate discuții pe aspecte privind condițiile legale de prelucrare a datelor în diferite domenii de activitate.

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

Prin intermediul site-ului Autorității s-a realizat o informare promptă și eficientă a persoanelor fizice, dar și a operatorilor, atât prin prisma celor **46 de comunicate de presă** postate la secțiunea „Știri", cât și a informațiilor de la secțiunea specială dedicată Regulamentului (UE) 679/2016.



Totodată, Autoritatea națională de supraveghere a continuat să publice amenzile dispuse în anul 2021, în baza Regulamentului (UE) 2016/679, raportat la caracterul public al activității desfășurate și într-o manieră similară cu abordarea celorlalte autorități naționale de protecția datelor din statele membre ale Uniunii Europene.

Pe de altă parte, operatorii din sectorul public și privat au continuat să declare **responsabilii cu protecția datelor**, în anul 2021 înregistrându-se la Autoritatea națională de supraveghere un număr de **2164** responsabili.

CAPITOLUL III

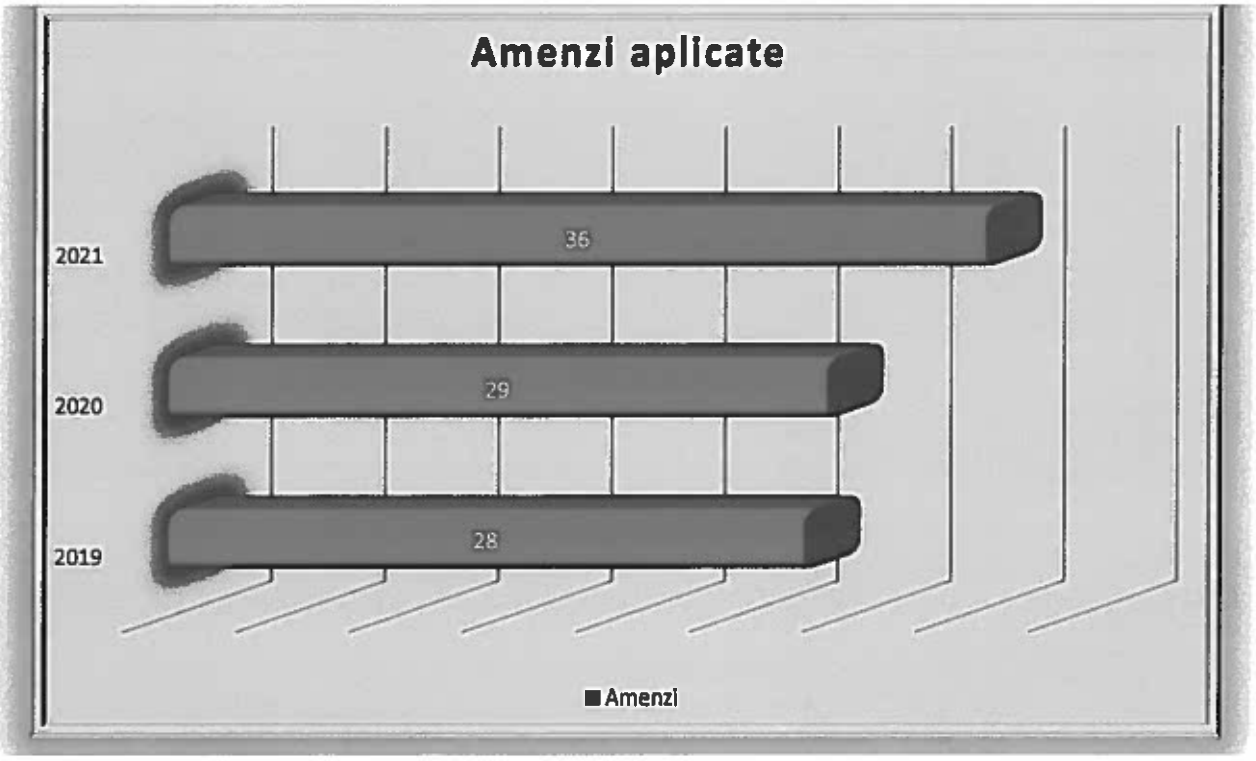
ACTIVITATEA DE MONITORIZARE ȘI CONTROL

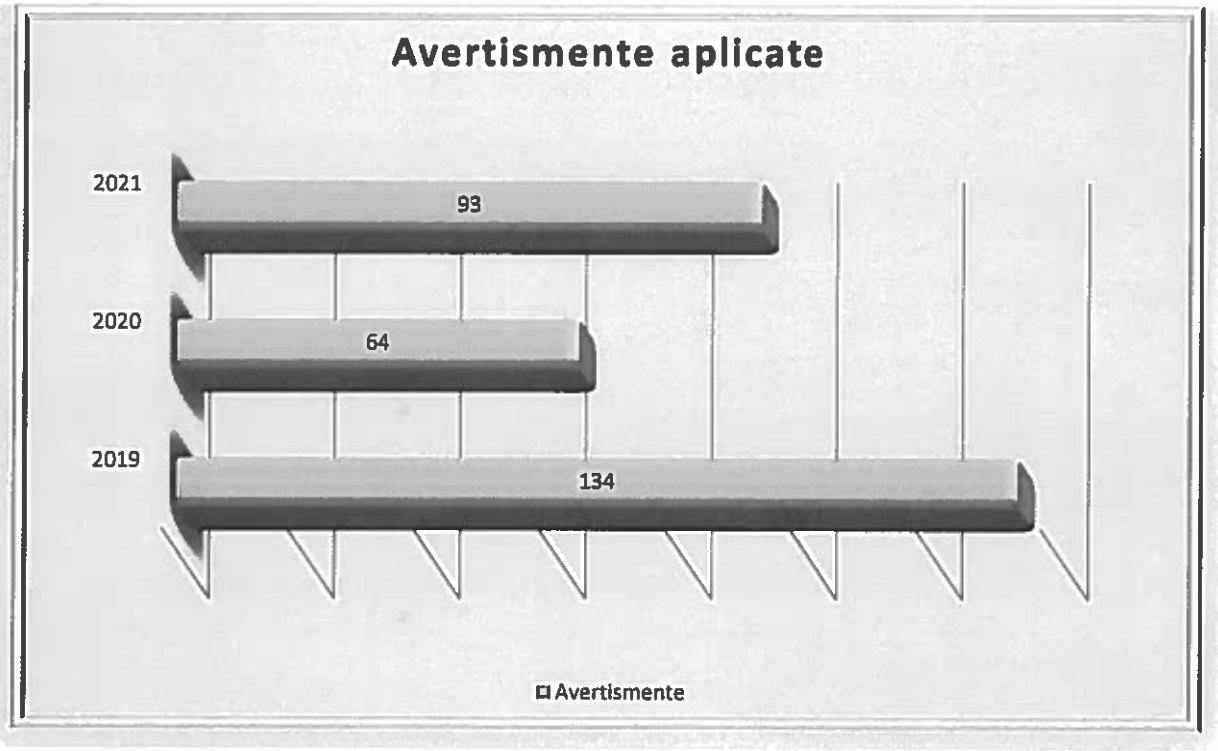
Secțiunea 1: Prezentare generală

În cursul anului 2021, Autoritatea națională de supraveghere a primit un număr de **5006** de plângeri, sesizări și notificări privind incidente de securitate, pe baza cărora au fost deschise **691** investigații.

Ca urmare a investigațiilor, au fost aplicate **36** de amenzi în cuantum total de **371.131,95** lei.

De asemenea, au mai fost aplicate **93** de avertismente și au fost dispuse **56** de măsuri corective și **1** avertizare.





În anul 2021, plângerile înregistrate la Autoritatea națională de supraveghere au vizat, în principal, următoarele aspecte:

- încălcarea drepturilor persoanelor vizate, în special, a dreptului de acces al persoanei vizate, de opoziție și a dreptului la ștergerea datelor acesteia;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video instalate de anagajatori la locul de muncă sau de asociațiile de proprietari în condominii;
- dezvăluirea datelor personale pe internet, inclusiv pe rețelele de socializare;
- prelucrarea datelor personale cu încălcarea prevederilor art. 6 din Regulamentul (UE) 2016/679 privind stabilirea corectă a temeiului legal ori lipsa acestuia;
- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date cu caracter personal;
- primirea de mesaje comerciale nesolicitate prin telefon sau poștă electronică.

Prin intermediul sesizărilor transmise în anul 2021 au fost semnalate, în principal, aspecte referitoare la:

- încălcarea drepturilor și a principiilor prevăzute de Regulamentul (UE) 2016/6792016/679;
- dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;

- publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele sociale;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video;
- primirea de mesaje comerciale nesolicitate;
- 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;
- raportarea de date personale la Biroul de Credit;
- lipsa măsurilor de securitate de tipul directory listing la nivelul website-urilor;
- utilizarea de camere video de tipul body-worn la nivelul poliției locale.

Referitor la incidentele de securitate transmise notificate de operatorii de date, acestea au vizat, în principal, următoarele aspecte:

- confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal afectate ca urmare a dezvăluirilor neautorizate ori ca urmare a unui software malițios, de tip ransomware;
- accesul ilegal la datele cu caracter personal ale clienților din sistemul bancar;
- accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV);
- dezvăluirea de date cu caracter personal în sistemul medical.

Secțiunea a 2 - a: Investigații din oficiu

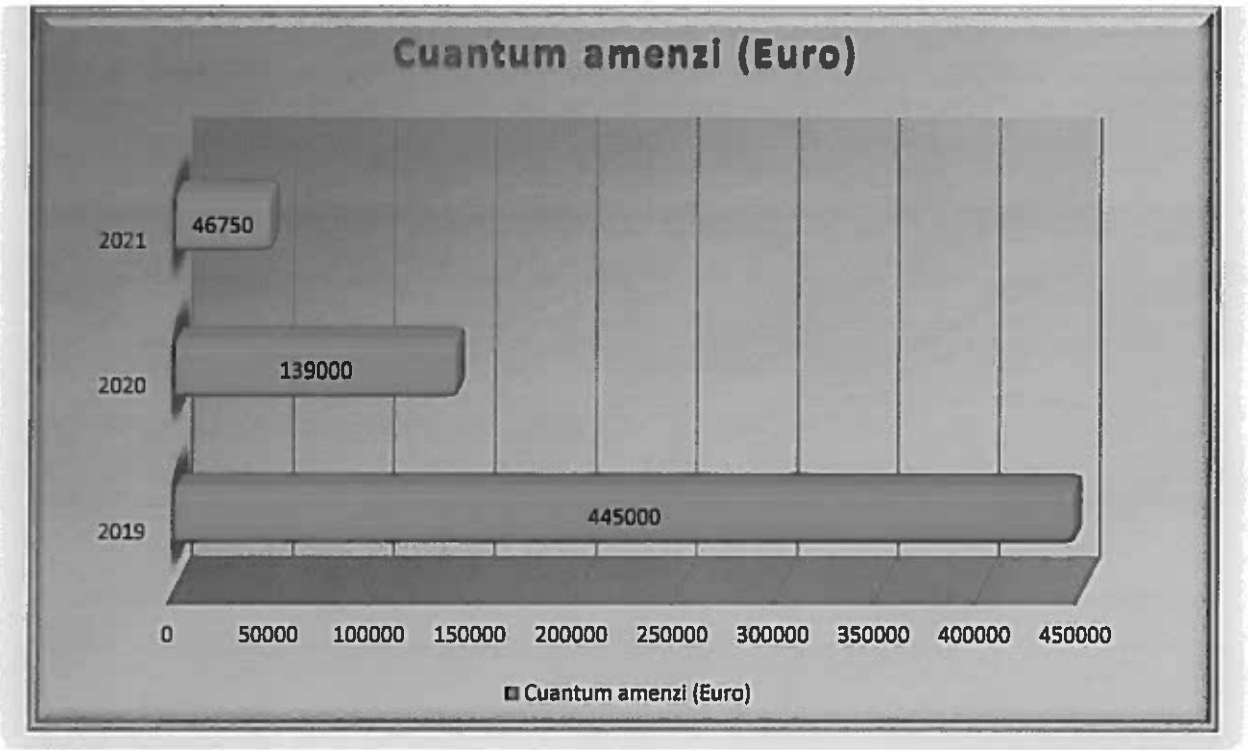
1. Prezentare generală

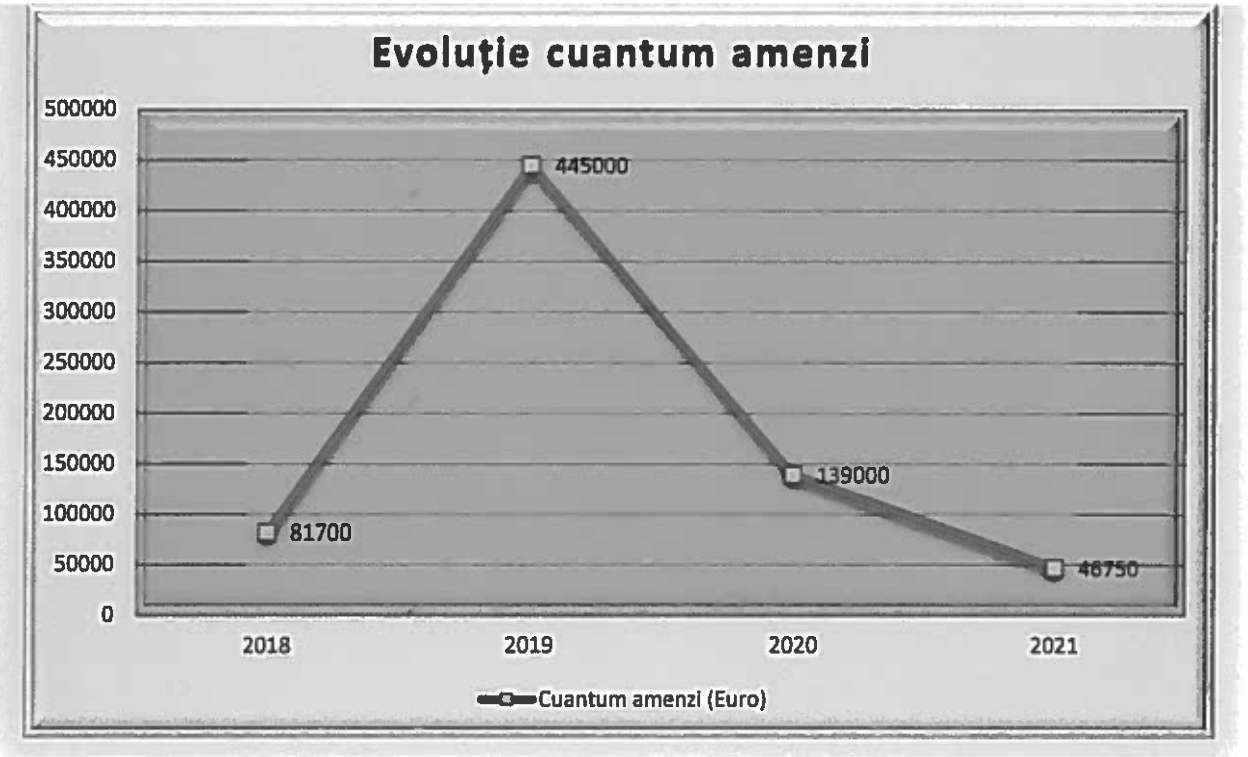
Și în cursul anului 2021, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea dispozițiilor Regulamentului (UE) 2016/679, ale Legii nr. 190/2018, dar și ale Legii nr. 506/2004, atât în sistemul public, cât și în cel privat.

În anul 2021, Autoritatea națională de supraveghere a primit un număr total de **372** de sesizări și notificări privind incidentele de securitate, dintre care **171** sesizări și **201** incidente de securitate.

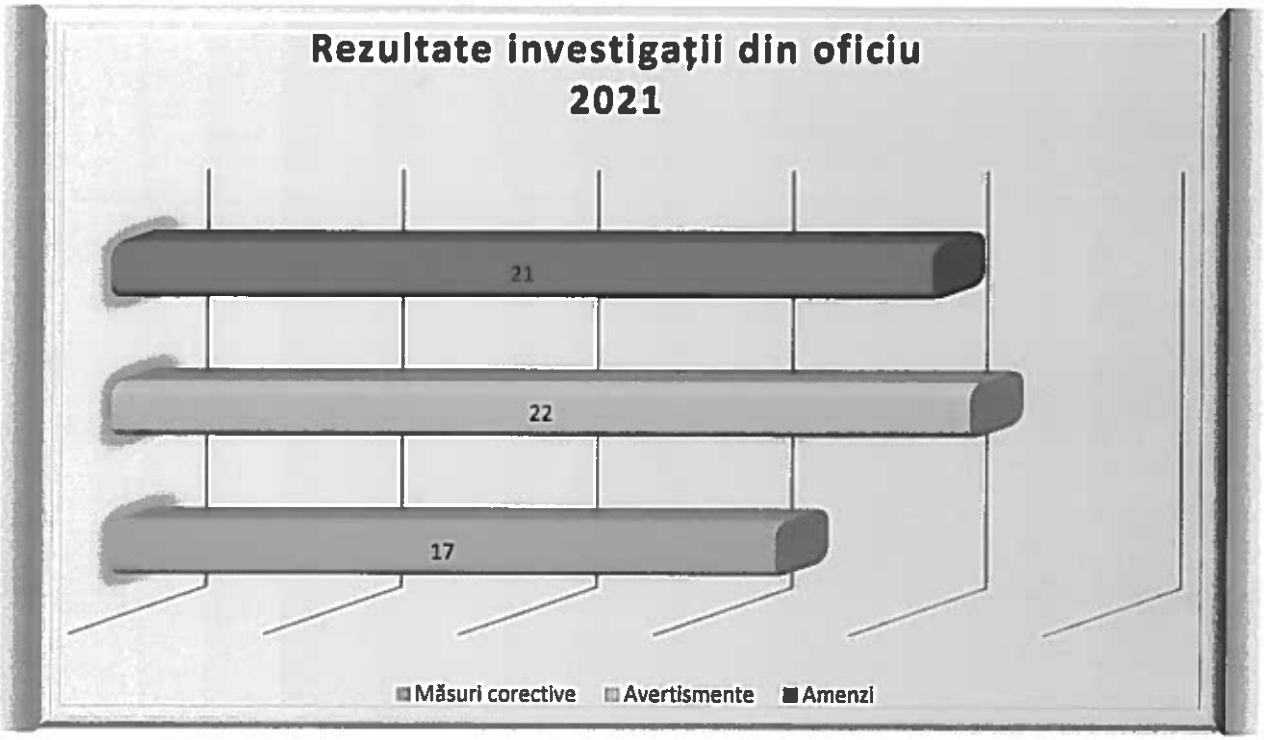
Pe baza sesizărilor și notificărilor privind incidentele de securitate au fost demarate verificări în vederea efectuării de investigații într-un număr de **372** de cazuri.

Ca urmare a investigațiilor efectuate, au fost aplicate **21** amenzi în cuantum total de **46750 euro**.





De asemenea, au fost aplicate **22** de avertismente și au fost dispuse **16** măsuri corective și **1** avertizare.



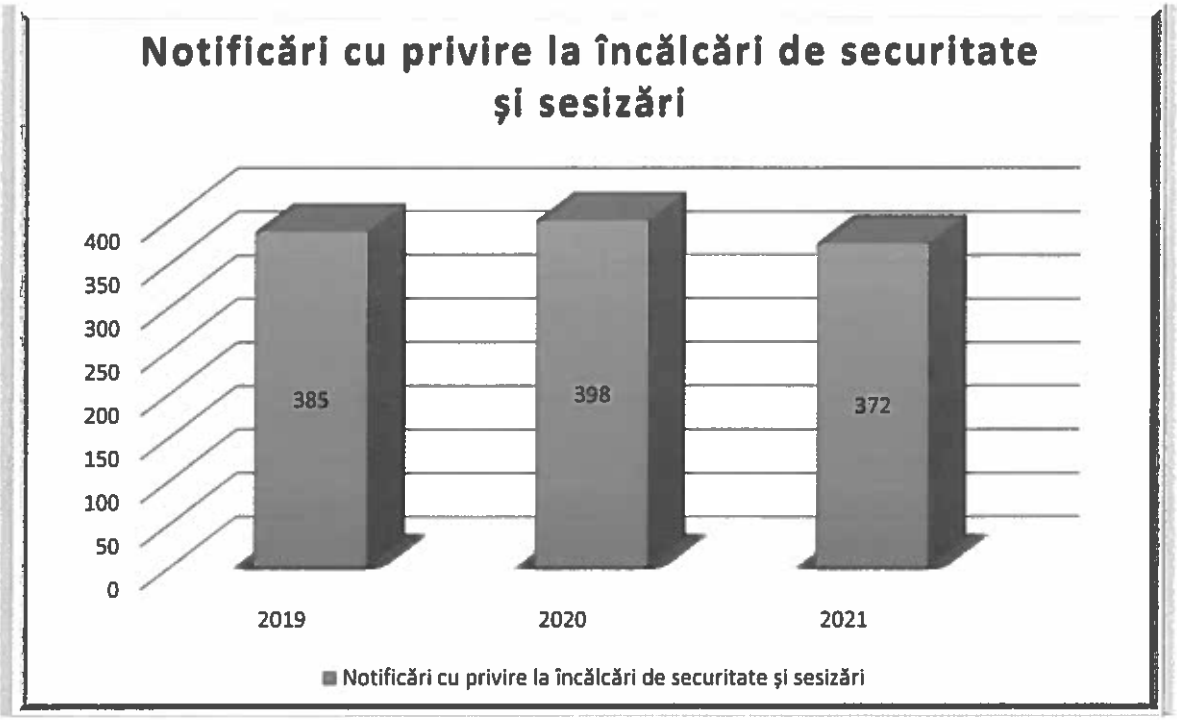
În anul 2021, prin intermediul sesizărilor transmise au fost semnalate, în principal, aspecte referitoare la:

- încălcarea drepturilor și a principiilor prevăzute de Regulamentul (UE) 2016/679;
- dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate;
- publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele sociale;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video;
- primirea de mesaje comerciale nesolicitate;
- 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;
- raportarea de date personale la Biroul de Credit;

- lipsa măsurilor de securitate de tipul directory listing la nivelul website-urilor;
- utilizarea de camere video de tipul body-worn la nivelul poliției locale.

Referitor la incidentele de securitate notificate de operatorii de date, acestea au vizat, în principal, următoarele aspecte:

- Confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal afectate ca urmare a dezvăluirilor neautorizate ori ca urmare a unui software malițios, de tip ransomware;
- Accesul ilegal la datele cu caracter personal ale clienților din sistemul bancar;
- Accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV);
- Dezvăluirea de date cu caracter personal în sistemul medical.



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

- ✓ Asigurarea conformității operațiunilor de prelucrare cu dispozițiile Regulamentului (UE) 2016/679;
- ✓ Respectarea principiilor de prelucrare a datelor, în special cele privind

legalitatea, transparența și proporționalitatea;

✓ Punerea în aplicare a unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător, cum ar fi verificarea periodică, prin sondaj, a datelor înregistrate în aplicațiile informatice, pentru a identifica accesările neautorizate;

✓ Instruirea personalului cu privire la măsurile luate de operator, astfel ca utilizatorii să aibă acces numai la datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu;

✓ Revizuirea şi actualizarea procedurilor de lucru referitoare la protecția datelor cu caracter personal.

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

În cursul anului 2021, sesizările referitoare la activitatea autorităților și organismelor publice au avut ca obiect, în principal, încălcarea măsurilor de securitate și confidențialitate, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal ale persoanelor vizate, inclusiv pe pagina de web sau pe rețelele de socializare, precum și prelucrarea excesivă a datelor cu caracter personal raportat la scopul prelucrării.

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

Totodată, Autoritatea națională de supraveghere a emis și o avertizare în atenția unui operator cu privire la posibilitatea ca operațiunile de prelucrare efectuate să încalce prevederile Regulamentului (UE) 2016/679.

Măsurile corective dispuse în urma investigațiilor au vizat, în special, următoarele: asigurarea conformității operațiunilor de prelucrare cu dispozițiile Regulamentului (UE) 2016/679, respectarea principiilor de prelucrare a datelor, instruirea personalului cu privire la măsurile luate de operator, astfel ca utilizatorii să aibă acces numai la datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu, precum și revizuirea şi actualizarea procedurilor de lucru referitoare la protecția datelor cu caracter personal.

În majoritatea cazurilor, autoritățile publice au îndeplinit măsurile corective dispuse, în termenul acordat de Autoritatea națională de supraveghere.

1. FIȘĂ DE CAZ – Accesul neautorizat la datele cu caracter personal ale petenților care au depus plângeri on-line pe pagina de internet a unei autorități publice locale

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că petițiile depuse on-line pe site-ul unei autorități publice locale pot fi vizualizate și descărcate de către oricine, prin accesarea unui link public.

Din investigația efectuată în acest caz, a rezultat că autoritatea publică în cauză nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, deși avea această obligație potrivit art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679, iar potrivit art. 5 alin. (1) lit. f) datele cu caracter personal trebuie prelucrate 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 („integritate şi confidenţialitate"). Aceasta a condus la accesul neautorizat la datele cu caracter personal (nume, prenume, domiciliu, e-mail) ale petenților care au depus on-line plângeri pe site-ul autorității publice și la divulgarea neautorizată a acestor date.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea art. 32 alin. (4), art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12 - 14 din Legea nr. 190/2018.

Astfel, în sarcina operatorului s-a dispus revizuirea şi actualizarea măsurilor tehnice şi organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, precum și revizuirea şi actualizarea procedurilor referitoare la serviciile electronice, astfel încât să fie evitate incidente similare de dezvăluire neautorizată a datelor cu caracter personal prelucrate.

Operatorul investigat a comunicat că a șters fișierul în cauză și a renunțat la serviciul on-line de pe site-ul său.

2. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal ale angajaților

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că un funcționar public din cadrul unei unități administrativ teritoriale a depus în instanță în cadrul unui litigiu de muncă, o copie după condica de prezență ce conținea datele personale ale angajaților.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că prelucrarea datelor cu caracter personal ale angajaților s-a efectuat fără consimțământul acestora sau fără un alt temei legal reglementat de art. 6 alin. (1) din Regulamentul (UE) 2016/679. Totodată, s-a constatat că operatorul investigat nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului. Aceasta a condus la pierderea confidențialității datelor cu caracter personal prelucrate, prin divulgarea neautorizată și accesul neautorizat la datele cu caracter personal (nume, prenume, normă, semnătură, ora venire, oră plecare, timp lucrat) ale angajaților proprii, prin xerocopierea unor pagini din condica de prezență a instituției și depunerea acestora la instanța de judecată, de către o angajată care se află într-un litigiu de muncă cu operatorul.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea art. 32 alin. (4), art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, dispunându-se revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea sa, în funcție de specificul activității, conform prevederilor Regulamentului (UE) 2016/679.

3. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal prin intermediul rețelelor de socializare

Autoritatea națională de supraveghere a fost sesizată cu privire la postarea pe contul unei persoane fizice, pe o rețea de socializare, a unui videoclip cu imagini înregistrate de sistemul de supraveghere video al unei autorități publice.

Din investigația efectuată în acest caz, a rezultat că operatorul investigat nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, deși avea această obligație potrivit art. 32 alin. (1) lit. b) și alin. 2) din Regulamentul (UE) 2016/679, iar datele cu caracter personal trebuie prelucrate 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 („integritate şi confidenţialitate"). Aceasta a condus la accesul neautorizat la date cu caracter personal (imagini) și la divulgarea neautorizată a acestora.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea a două măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12 - 14 din Legea nr. 190/2018.

Astfel, în sarcina operatorului s-a dispus:

- revizuirea şi actualizarea măsurilor tehnice şi organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor pentru protejarea datelor personale colectate prin intermediul sistemului de supraveghere video;

- stabilirea unor instrucțiuni clare de prelucrare a imaginilor video, stocate în sistemul de supraveghere video, pentru persoanele care prelucrează aceste date sub autoritatea operatorului, astfel încât să se evite accesarea, diseminarea sau prelucrarea în alt mod neautorizat a acestora.

4. FIȘĂ DE CAZ – Divulgarea neautorizată și accesul neautorizat la datele cu caracter personal prelucrate de către o autoritate publică locală pe pagina de internet

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, pe site-ul Ghidul Primăriilor, a fost publicată o listă a datornicilor persoane fizice dintr-o comună, chiar dacă datoriile acestora erau stinse. Lista publicată cuprindea următoarele date cu caracter personal: nume, prenume, adresă, stradă și număr de casă.

S-a solicitat operatorului, în cadrul investigației efectuate, informații cu privire la circumstanțele concrete în care au fost dezvăluite datele cu caracter personal din lista datornicilor, precum și informații cu privire la respectarea prevederilor Regulamentului General privind Protecția Datelor.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea art. 58 alin. (1) lit. a) și lit. e) din Regulamentul (UE) 2016/679, în temeiul art. 13 din Legea nr. 190/2018, deoarece nu a răspuns solicitărilor Autorității naționale de supraveghere.

Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12 - 14 din Legea nr. 190/2018. Astfel, în sarcina operatorului s-a dispus furnizarea tuturor informațiilor solicitate de către Autoritatea națională de supraveghere în vederea îndeplinirii sarcinilor sale.

Ca urmare a emiterii procesului-verbal de către Autoritatea națională de supraveghere, operatorul a transmis informațiile necesare pentru soluționarea cazului și a șters de pe site lista cu datornicii persoane fizice ale căror datorii erau stinse.

5. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal pe contul unei autorități publice, de pe o rețea de socializare

Autoritatea națională de supraveghere s-a sesizat din oficiu, ca urmare a apariției în mass-media a unor informații privind o posibilă încălcare a dispozițiilor Regulamentului (UE) 2016/679 prin divulgarea, pe contul de pe o rețea de socializare al unei autorități publice, datelor cu caracter personal (nume, prenume și domiciliu) ale persoanelor izolate la domiciliu în contextul pandemiei de COVID-19.

Din investigația efectuată în acest caz, a rezultat că autoritatea publică a prelucrat date cu caracter personal cu încălcarea art. 6 alin. (1) din Regulamentul (UE) 2016/679, fără

consimțământul persoanelor vizate sau fără alt temei legal prevăzut de Regulamentul (UE) 2016/679 și a încălcat prevederile art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679 deoarece nu a informat persoanele vizate izolate la domiciliu, ale căror date personale le-a prelucrat prin postarea/publicarea/divulgarea pe contul său de pe o rețea de socializare, în scopul protejării sănătății localnicilor în contextul pandemiei de COVID-19.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea art. 5 alin. 1 lit. a) și art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12 - 14 din Legea nr. 190/2018.

Astfel, în sarcina operatorului s-a dispus luarea unor măsuri astfel încât să fie evitate prelucrările nelegale ale datelor cu caracter personal, fără existența unui temei legal clar determinat, cu respectarea principiilor și a condițiilor de legalitate prevăzute de Regulamentul (UE) 2016/679.

6. FIȘĂ DE CAZ – Prelucrarea excesivă a datelor, raportat la scopurile prelucrării

Autoritatea națională de supraveghere a fost sesizată cu privire la o posibilă încălcare a prevederilor Regulamentului (UE) 2016/679, referitoare la prelucrarea datelor cu caracter personal ale persoanelor fizice posesoare de permise de acces auto, într-o anumită zonă rezidențială.

În fapt, prin intermediul unui Regulament de acces auto în Zona Peninsulară, aprobat printr-o hotarâre a consiliului local, o autoritate publică prevedea că accesul rezidenților se va putea efectua doar în baza unui permis de acces eliberat de către Primărie, în care vor fi trecute atât numele posesorului auto, cât și adresa acestuia. Permisul de acces trebuia expus în bordul autoturismului, la vedere.

Din investigația efectuată în acest caz, Autoritatea națională de supraveghere a constatat că până la data efectuării investigației, operatorul nu a efectuat operațiuni de prelucrare a datelor cu caracter personal conform prevederilor Regulamentului de acces auto.

Autoritatea națională de supraveghere a mai constatat faptul că prin operațiunile de prelucrare prevăzute în scopul emiterii permiselor de acces auto pentru rezidenții persoane fizice în Zona Peninsulară, conform prevederilor hotărârii consiliului local, există posibilitatea ca operatorul să încalce principiul "reducerii la minimum a datelor" prevăzut de art. 5 alin.

(1) lit. c) din Regulamentul (UE) 2016/679, deoarece datele cu caracter personal colectate și dezvăluite pe talonul permisului de acces auto în Zona Peninsulară, afișat în bordul autoturismului, respectiv numele și prenumele titularului, numărul autoturismului și perioada de valabilitate, nu sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate.

Autoritatea națională de supraveghere a emis *o avertizare* în atenția operatorului, 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.

Totodată, a fost dispusă și măsura corectivă constând în luarea de măsuri în vederea respectării principiului "reducerii la minimum a datelor" prevăzut de art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679, în ceea ce privește prelucrarea datelor cu caracter personal în scopul emiterii permiselor de acces auto pentru rezidenții persoane fizice în Zona Peninsulară (de ex. utilizarea unor identificatori care să permită identificarea indirectă a persoanei vizate cum ar fi nr. cererii), inclusiv prin modificarea prevederilor hotărârii de consiliu local, referitor la această prelucrare.

7. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal prin publicarea în Monitorul Oficial de către o autoritate publică centrală

O autoritate publică centrală a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului privind încălcarea securității datelor cu caracter personal, aprobat prin Decizia nr. 128/2018 privind aprobarea formularului tipizat al notificării de încălcare a securității datelor cu caracter personal în conformitate cu Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor). Acesta a constat în publicarea dintr-o eroare, în Monitorul Oficial, a unei anexe la un ordin de ministru, ce conținea o listă cu locul de muncă și numerele de telefon a 1206 persoane vizate.

Autoritatea națională de supraveghere a constatat în cadrul investigației desfășurate că, pentru 283 persoane vizate dintre cele 1206 notificate inițial, datele cu caracter personal/numere de telefon, publicate în Monitorul Oficial, au fost divulgate neautorizat.

Autoritatea națională de supraveghere a mai constatat că autoritatea publică în cauză nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

Aceasta a condus la divulgarea neautorizată a datelor cu caracter personal a persoanelor vizate, prin publicarea în Monitorul Oficial a unui ordin de ministru, fapt ce poate duce în special la prejudicii fizice, materiale sau morale aduse persoanelor fizice afectate, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau pierderea confidenţialităţii datelor cu caracter personal protejate prin secret profesional sau alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12 - 14 din Legea nr. 190/2018.

Astfel, în sarcina operatorului s-a dispus implementarea de măsuri tehnice şi organizatorice, inclusiv proceduri de lucru referitoare la protecția datelor cu caracter personal, precum și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea sa, inclusiv în ceea ce privește fluxul operațiunilor privind transmiterea de ordine, instrucțiuni și alte acte cu caracter normativ în vederea publicării în Monitorul Oficial.

Operatorul a transmis Autorității naționale de supraveghere o adresă prin care a menționat că a implementat două proceduri de sistem privind prelucrarea datelor cu caracter personal și privind raportarea și tratarea incidentelor de sucuritate, a precizat că trimestrial va realiza o instruire a personalului, iar fiecare șef de structură va întreprinde măsuri de implementare proprii structurii, inclusiv întocmirea de proceduri operaționale concrete, urmând ca toate structurile care operează cu date cu caracter personal în fluxul operațiunilor privind transmiterea de ordine, instrucțiuni și alte acte cu caracter normativ în vederea publicării în Monitorul Oficial al României sau alte publicații să obțină și avizul responsabilului cu protecția datelor de la nivelul operatorului.

8. FIȘĂ DE CAZ – Prelucrarea datelor cu caracter personal prin intermediul sistemelor audio-video de tip body-worn camera

Autoritatea națională de supraveghere a fost sesizată cu privire la obligația polițiștilor locali, din cadrul unei direcții generale de poliție locală, de a purta asupra lor pe întreaga durată a timpului de lucru camere de înregistrare audio-video de tip body – worn camera.

În cadrul investigației Autorității naționale de supraveghere, operatorul a declarat că obiectivele camerelor de înregistrare audio - video de tip body – worn camera sunt orientate către persoanele care săvârșesc acte antisociale ori către persoanele aflate în dificultate și care necesită acordarea ajutorului de urgență, iar scopul utilizării acestor sisteme este protecția polițiștilor locali împotriva faptelor de ultraj și a acuzațiilor îndreptate împotriva acestora, cu privire la modul de exercitare a atribuțiilor de serviciu și de protecție a persoanelor ce fac obiectul intervențiilor și acțiunilor acestora și de descurajare a săvârșirii unor fapte ilegale, ca urmare a conștientizării faptului că intervențiile și acțiunile polițiștilor locali sunt înregistrate.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că temeiurile legale invocate de către operatori nu conțin dispoziții care să reglementeze utilizarea unor sisteme de supraveghere audio – video portabile în activitatea polițiștilor locali.

Totodată, s-a constatat că prelucrarea datelor cu caracter personal (imagine, voce) s-a efectuat cu încălcarea art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679 și fără îndeplinirea condițiilor de legalitate a prelucrării, așa cum sunt prevăzute în art. 6 alin. (1) din Regulamentul (UE) 2016/679, deși operatorul avea obligația de a prelucra datele în mod legal, echitabil și transparent față de persoanele vizate.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea art. 5 alin. (1) lit. a) raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679.

Sancțiunea avertismentului a fost însoțită de aplicarea unor măsuri corective, prin planul de remediere, de a asigura conformitatea operațiunilor de prelucrare efectuate prin utilizarea sistemelor audio-video portabile cu dispozițiile art. 5 și art. 6 din Regulamentul (UE) 2016/679.

Totodată, Autoritatea națională de supraveghere a dispus, prin decizie, încetarea oricăror operațiuni sau set de operațiuni de prelucrare a dator cu caracter personal efectuate prin intermediul sistemelor audio-video de tip body – worn camera și ștergerea sistemului

de evidență a datelor cu caracter personal constituit ca urmare a utilizării unor astfel de sisteme.

9. FIȘĂ DE CAZ - Divulgarea neautorizată și accesul neautorizat la datele cu caracter personal ale studenților prin accesarea unor linkuri ale web-site-ului unei instituții de învățământ public

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, prin accesarea anumitor link-uri de pe site-ul unei instituții publice de învățământ superior, pot fi vizualizate și descărcate documente ale studenților universității, ce conțineau date cu caracter personal (cărți identitate, certificate de naștere, adeverințe medicale, contracte, burse, cazare, etc.).

Autoritatea națională de supraveghere a efectuat o investigație în urma căreia a constatat că, după luarea la cunoștință a incidentului, instituția de învățământ a blocat accesul la paginile web unde puteau fi vizualizate și descărcate datele și a scanat și analizat întreg website-ul. De asemenea, s-a stabilit că la conținutul folderelor și subfolderelor din link-uri unde puteau fi vizualizate și/sau descărcate date cu caracter personal, vor avea acces doar persoanele autorizate din cadrul facultății. Astfel, accesul la datele cu caracter personal se va face pe bază de autentificare (cu nume utilizator, parolă), informațiile nefiind publice.

Autoritatea națională de supraveghere a mai constatat că instituția publică de învățământ superior în cauză a încălcat prevederile art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679, deoarece nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod. Aceasta a condus la încălcarea regulilor privind confidențialitatea datelor cu caracter personal, prin accesarea link-urilor care conțin foldere și subfoldere cu datele cu caracter personal ale studenților (nume, prenume, CNP, număr de telefon, adresă de e-mail, etc., cuprinse în cărți identitate, adverințe medicale, contracte de studii universitare, etc.).

Autoritatea națională de supraveghere, în temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 16 alin. (5) din Legea nr. 102/2005, a dispus o măsură corectivă împotriva operatorului instituție publică de învățământ

superior, respectiv instruirea angajaților asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale prelucrate.

B. Investigații referitoare la prelucrarea datelor cu caracter personal de către entități din domeniul financiar-bancar și societăți de asigurare

În anul 2021, investigațiile din oficiu la entitățile din domeniul financiar-bancar și societățile de asigurare, s-au desfășurat ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal, precum și a sesizărilor cu privire la prelucrarea datelor cu caracter personal.

Notificările de încălcare a securității datelor cu caracter personal au avut ca obiect, în principal: divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal prelucrate, neimplementarea unor măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare, neimplementarea unor măsuri pentru a asigura faptul că orice persoană fizică care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului.

Sesizările au avut ca obiect, în principal, divulgarea neautorizată a datelor cu caracter personal. Totodată, au existat situații în care încălcarea securității datelor cu caracter personal a avut loc ca urmare a neimplementării măsurilor tehnice și organizatorice adecvate de către persoana împuternicită de către operator.

În urma investigațiilor efectuate au fost aplicate sancțiuni contravenționale și măsuri corective, atât operatorilor cât și împuterniciților acestora.

1. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal de către o instituție financiar – bancară

O instituție financiar-bancară a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018.

În fapt, instituția financiar-bancară a transmis către un partener contractual în vederea emiterii unor polițe de asigurare, două fișiere conținând atât informații corecte, cât și informații inexacte sau neactualizate. Fișierele transmise conțineau date cu caracter personal aferente unui număr de 270 de persoane vizate (nume și prenume, cod numeric personal, naționalitate, adresă domiciliu, adresă imobil asigurat, telefon, adresă e-mail, CIF - cod identificare client, Cod IBAN, tip de credit asociat poliței de asigurare, număr contract credit).

Autoritatea națională de supraveghere a constatat, în investigația efectuată în acest caz, că angajații departamentului de monitorizare a polițelor de asigurare, din cadrul instituției financiar-bancare, nu au verificat și procesat polițele de asigurare în conformitate cu Procedura de lucru, astfel încât informațiile utilizate în cadrul procesului de emitere a unor noi polițe de asigurare nu au fost actualizate (polițele de asigurare transmise pe e-mail nu au fost înregistrate în sistemul central al Băncii).

Incidentul de securitate a afectat un număr de 270 de persoane fizice vizate, producând și efecte financiare asupra acestora. Ca urmare, instituția bancară a inițiat un proiect intern care are în vedere automatizarea procesului, simplificarea pașilor parcurși și includerea unor măsuri adiționale de verificare.

Autoritatea națională de supraveghere a constatat, la data efectuării investigației, că instituția financiar-bancară nu a luat suficiente măsuri pentru a se 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. Astfel, neimplementarea unor măsuri tehnice și organizatorice adecvate înainte de producerea incidentului, au condus la încălcarea confidențialității datelor cu caracter personal, prin divulgare neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod, prin transmiterea a două fișiere, care conțineau date cu caracter personal, către un partener contractual, în vederea emiterii unor polițe de asigurare, fișiere care conțineau atât informații corecte cât și informații inexacte sau neactualizate.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 4.874,40 lei (echivalentul a 1000 EURO), pentru încălcarea prevederilor art. 29, art. 32 alin. (2) și art. 32 alin. (4) din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ – Distrugerea datelor cu caracter personal ale clienților unei societăți financiar-bancare de către angajatul persoanei împuternicite de operator

O instituție financiar-bancară a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018, care a constat în faptul că împuternicitul pentru prelucrarea datelor cu caracter personal nu a predat instituției financiar-bancare documentele aferente activităților de prescoring, efectuate de un angajat al său, pe motiv că acestea au fost distruse.

Autoritatea națională de supraveghere a fost sesizată, în același timp, de către o persoană fizică, cu privire la faptul că o societate comercială (împuternicită pentru prelucrarea datelor cu caracter personal de către instituția financiar-bancară anterior menționată) solicită ca agenții de vânzare să arhiveze datele clienților societății financiar-bancare pe care le prelucrează, deși aceștia își exprimă în mod expres opoziția conform legislației în vigoare. De asemenea, persoana fizică a sesizat că, prin parola de acces la sistemul societății financiar - bancare, agenții de vânzări pot vizualiza datele personale ale clienților din toată țara, fără drept și fără acordul băncii beneficiare sau al respectivilor clienți.

Autoritatea națională de supraveghere a efectuat o investigație la persoana împuternicită de operator și la data efectuării investigației a constatat că, urmare a efectuării a 1372 de prescoringuri de către un agent de vânzări, angajat al persoanei împuternicite de către instituția financiar-bancară, au fost afectate de incidentul de securitate 1058 de persoane fizice vizate, întrucât documentația originală aferentă prescoringurilor nu a fost predată de agent, ci distrusă, ceea ce a generat incidentul de securitate notificat de către instituția financiar-bancară.

Totodată, s-a constatat că societatea împuternicită pentru prelucrarea datelor cu caracter personal nu a luat măsuri pentru a se asigura că orice persoană fizică care acționează sub autoritatea sa și care are acces la date cu caracter personal nu le prelucrează decât la cererea sa și nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un

alt mod. Aceasta a condus la distrugerea datelor cu caracter personal ale clienților unei societăți financiar-bancare, de către un angajat al persoanei împuternicite de către societatea financiar-bancară menționată anterior.

Autoritatea națională de supraveghere a sancționat societatea împuternicită pentru prelucrarea datelor cu caracter personal cu amendă în cuantum de 7.331,85 lei (echivalentul a 1500 EURO), pentru încălcarea prevederilor art. 29, art. 32 alin. (2) și art. 32 alin. (4) din Regulamentul (UE) 2016/679.

3. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal de către o societate de asigurări

Autoritatea națională de supraveghere a fost sesizată de către o persoană fizică, cu privire la faptul că a primit un e-mail din partea unei societăți de asigurări, care conținea o listă cu datele cu caracter personal din dosarele de daună ale unui număr de 54 de persoane vizate.

La data efectuării investigației, s-a constatat că societatea de asigurări nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, ceea ce a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal (nume, prenume și adresă de domiciliu) ale unui număr de 45 de persoane fizice, precum și numele și prenumele, în cazul celei de-a 46-a persoane.

Autoritatea națională de supraveghere a dispus împotriva operatorului controlat, în temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, o măsura corectivă referitoare la revizuirea şi actualizarea măsurilor tehnice şi organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor referitoare la comunicațiile electronice, precum și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea sa, referitoare la obligațiile ce le revin conform prevederilor Regulamentul (UE) 2016/679.

C. Investigații referitoare la prelucrarea datelor cu caracter personal în domeniul sănătății

În cursul anului 2021, sesizările și notificările încălcărilor de securitate cu privire la prelucrarea datelor cu caracter personal în domeniul sănătății au avut ca obiect, în principal, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal ale persoanelor vizate (pacienți).

Investigațiile efectuate de către Autoritatea națională de supraveghere au vizat prelucrarea datelor cu caracter personal efectuate atât de către entități medicale din sectorul public (spitale), cât și de entități medicale din sectorul privat.

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

În majoritatea cazurilor, operatorii investigați au îndeplinit măsurile de remediere dispuse, în termenul acordat de Autoritatea națională de supraveghere.

FIȘĂ DE CAZ - Divulgarea și accesul neautorizate la datele cu caracter personal ale pacienților unui furnizor de servicii medicale

Un furnizor de servicii medicale a notificat Autoritatea națională de supraveghere cu privire la producerea mai multor incidente de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018, astfel:

1) Transmiterea eronată a răspunsului către o persoană vizată/client, la o adresă de e-mail care aparținea altei persoane. Un angajat al furnizorului de servicii medicale a utilizat pentru transmiterea răspunsului, adresa scrisă olograf de către persoana vizată pe formularul de reclamație. Deoarece răspunsul transmis inițial s-a întors automat la expeditor cu mențiunea că "adresa de e-mail nu există", răspunsul a fost retransmis pe o adresă de e-mail secundară, identificată în sistemul informatic al furnizorului de servicii medicale, care fusese furnizată anterior de către client, într-un alt scop.

E-mailul transmis eronat conținea numele pacientei și informații din care se puteau deduce starea de sănătate.

Deținătoarea adresei de e-mail utilizate pentru furnizarea răspunsului a semnalat faptul că a redirecționat mesajul către destinatarul corect, iar persoana vizată a sesizat faptul că au fost dezvăluite date confidențiale unei alte persoane.

2) Transmiterea prin e-mail a unui contract de prestări servicii medicale către o altă persoană decât titularul de contract, dintr-o eroare umană. Contractul a fost transmis în mod securizat (prin criptare cu parolă).

3) Transmiterea prin curier, a unui plic conținând un contract al unui viitor client al clinicii, împreună cu un alt contract aparținând unui alt client. Clientul care a primit, în mod eronat, contractul ce nu îi era adresat, a sesizat clinica și a predat contractul.

Urmare a investigațiilor efectuate în aceste cazuri, Autoritatea națională de supraveghere a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucrează decât la cererea operatorului. Aceasta a condus la divulgarea neautorizată a datelor prelucrate (nume și prenume, CNP, serie și nr. CI, adresă CI, adresa de corespondență, telefonul de contact și e-mail, respectiv nume și date privind starea de sănătate).

Totodată, Autoritatea națională de supraveghere a constatat că divulgarea neautorizată a datelor personale prelucrate poate duce în special la prejudicii materiale sau morale aduse persoanelor fizice afectate, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 9749,6 lei (echivalentul a 2000 EURO), pentru încălcarea art. 32 alin. (4), art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul General privind Protecția Datelor.

Totodată, au fost dispuse și două măsuri corective, constând în:

- revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal, precum și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea sa, referitor la obligațiile ce le revin conform prevederilor Regulamentului (UE) 2016/679, inclusiv cu

privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii;

- identificarea și implementarea unor măsuri pentru a se asigura că datele cu caracter personal prelucrate sunt exacte și actualizate, având în vedere scopurile pentru care sunt prelucrate, iar cele inexacte sunt şterse sau rectificate fără întârziere (spre exemplu, un mecanism de verificare a validității adresei de e-mail la momentul colectării).

Operatorul a comunicat Autorității naționale de supraveghere care au fost demersurile întreprinse de acesta ca urmare a măsurilor corective aplicate, respectiv revizuirea procedurilor privind prelucrarea datelor cu caracter personal, precum și instruirea angajaților.

D. Investigații referitoare la prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice

În cursul anului 2021, furnizorii de servicii de telecomunicații au notificat producerea unor incidente de încălcare a securității datelor cu caracter personal, atât prin completarea formularului aprobat prin Decizia nr. 128/2018, cât și prin completarea formularului privind încălcarea securității datelor cu caracter personal pentru furnizorii de servicii publice de rețele sau servicii de comunicații electronice, adoptat prin Decizia nr. 184/2014 privind aprobarea formularului tipizat al notificării de încălcare a securităţii datelor cu caracter personal pentru furnizorii de servicii publice de reţele sau servicii de comunicaţii electronice, în conformitate cu Regulamentul (UE) nr. 611/2013 al Comisiei din 24 iunie 2013 privind măsurile aplicabile notificării încălcărilor securităţii datelor cu caracter personal în temeiul Directivei 2002/58/CE a Parlamentului European şi a Consiliului privind confidenţialitatea şi comunicaţiile electronice.

Obiectul incidentelor de încălcare a securității datelor cu caracter personal notificate de către furnizorii de servicii de telecomunicații au fost, în principal, următoarele: transmiterea către destinatari eronați prin e-mail/SMS/poștă a facturilor/notificărilor de plată/contractelor/cereri de portare număr telefonie mobilă a unor clienți, accesarea ilicită a datelor cu caracter personal a unor clienți și pierderea temporară asupra disponibilității datelor clienților, accesarea ilicită a datelor cu caracter personal aferente unui număr de telefon al unui client în scopul migrării numărului de telefon de la un serviciu preplătit la un

serviciu postplătit (abonament) pe numele altui utilizator/client decât cel care deținea de fapt acel număr număr de SIM.

În majoritatea cazurilor, operatorii investigați au îndeplinit măsurile de remediere dispuse, în termenul acordat de Autoritatea națională de supraveghere.

1. FIȘĂ DE CAZ - Divulgarea și accesul neautorizate la datele cu caracter personal ale clienților unui furnizor de servicii de telecomunicații

Un furnizor de servicii de telecomunicații a notificat Autoritatea națională de supraveghere cu privire la producerea mai multor incidente de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018, cât și prin completarea formularului aprobat prin Decizia nr. 184/2014.

a) Încălcările de securitate notificate prin completarea formularului aprobat prin Decizia nr. 128/2018 au avut ca obiect: divulgarea datelor cu caracter personal ale unui client prin transmiterea contractelor de servicii încheiate cu un terț la o adresă eronată de e-mail, pentru obținerea de telefoane în mod fraudulos, dezvăluirea datelor cu caracter personal ale unui client prin transmiterea unei copii a contractului către un terț, prin intermediul e-mailului, accesul neautorizat la datele cu caracter personal ale unor clienți, în scop personal, dezvăluirea datelor cu caracter personal ale unui client prin transmiterea de facturi detaliate unei terțe persoane, accesare nelegală a datelor cu caracter personal în conturile mai multor clienți; accesare neautorizată și dezvăluirea datelor cu caracter personal ale unui client către un terț.

Datele cu caracter personal afectate de incidentele de securitate au fost următoarele: nume persoană de decizie, număr de contact, data activării serviciului, nume și prenume, email, cetățenie, serie și nr. act de identitate, adresă, număr cartelă SIM, identificatori pentru client, valoare reîncărcată, ofertă curentă, data și ora efectuării apelurilor facturate, numerele apelate, detalii legate de tipul evenimentului (roaming, date, voce, SMS), durata apelurilor, costul apelurilor, oferta activă în contul clientului, identificatori pentru contul clientului și pentru evenimentele înregistrate, CNP, numărul de telefon.

Autoritatea națională de supraveghere, în urma investigației efectuate, a sancționat operatorul cu amendă în cuantum de 7.421,25 lei (echivalentul a 1500 EURO), pentru încălcarea prevederilor art. 32 alin. (1) lit. b) și alin. (4) din Regulamentul General privind Protecția Datelor.

b) Încălcările de securitate notificate prin completarea formularului adoptat prin Decizia nr. 184/2014 au avut ca obiect: accesarea ilicită a datelor cu caracter personal în scopul închiderii serviciilor aferente unui număr de telefon de pe contul unui client, accesarea ilicită a datelor cu caracter personal și transmiterea acestora către alte adrese de e-mail decât cele ale titularilor, accesarea ilicită a datelor cu caracter personal prin înlocuirea SIM-ului unui client la solicitarea soției acestuia din urmă, limitând accesul clientului la numărul său de telefon, accesarea ilicită a datelor cu caracter personal ale unui număr de clienți, prin activări multiple și retenții de date pentru scopul de operațiuni de activare de servicii cu achiziții de dispozitive și de operațiuni de resemnare de servicii cu achiziție de dispozitiv, accesarea ilicită a datelor cu caracter personal și dezvăluirea de informații detaliate ale unui angajat al societății către un terț.

La data efectuării investigației, Autoritatea națională de supraveghere a constatat că operatorul nu a luat măsuri tehnice și organizatorice adecvate în vederea asigurării securității prelucrării datelor cu caracter personal. Aceasta a condus la prelucrarea și accesarea ilicită a datelor cu caracter personal (numărul de telefon, data și ora efectuării apelurilor facturate, numerele apelate, durata apelurilor, costul apelurilor, oferta activă în contul clientului, detalii legate de tipul evenimentului (roaming, date, voce, SMS), identificatori pentru client, pentru contul clientului și pentru evenimentele înregistrate, data și ora efectuării apelurilor facturate, nume, prenume, adresă, CNP, seria și numărul actului de identitate, cetățenia, numărul de telefon de contact, numărul de telefon, numărul de cartelă SIM și data activării serviciului) ale unui număr de 64 de persoane vizate.

Autoritatea națională de supraveghere, în urma investigației efectuate, a sancționat operatorul cu amendă în cuantum de 7000 lei, pentru încălcarea art. 3 alin. (1) și alin. (3) lit. a) și b) din Legea nr. 506/2004, modificată și completată.

2. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal ale minorilor prin intermediul unei platforme on-line

O societate comercială a notificat Autoritatea națională de supraveghere cu privire la producerea unui incident de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018, ca urmare a organizării unui concurs de desene, la care au participat copiii angajaților societății.

În fapt, persoanele vizate au încărcat în platforma on-line dedicată, desenele împreună cu formularul de participare la concurs, care conținea date cu caracter personal, ale minorilor și ale părintelui/tutorelui legal, precum și consimțământul acestuia.

Pentru votarea celui mai bun desen, pe platforma on-line dedicată, au fost publicate, din eroare, desenele copiilor împreună cu datele cu caracter personal cuprinse în formularul de participare: numele, prenumele și vârsta minorilor, numele, prenumele, orașul, țara, e-mailul, numărul de marcă al angajaților societății și semnătura olografă a părintelui/tutorelui legal.

Autoritatea națională de supraveghere a constatat în cadrul investigației efectuate, că operatorul nu a implementat măsuri tehnice și organizatorice adecvate pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la datele cu caracter personal nu le prelucrează decât la cererea operatorului cu excepția cazului în care această obligație îi revine în dreptul Uniunii sau dreptului intern și în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării, incluzând capacitatea de a asigura confidențialitatea datelor. Aceasta a condus la divulgarea neautorizată și/sau accesul neautorizat la datele cu caracter personal ale minorilor și angajaților proprii.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 4948.80 lei (echivalentul a 1000 EURO), pentru încălcarea dispozițiilor art. 32 alin. (1) lit. b) și art. 32 alin. (2) din Regulamentul General privind Protecția Datelor.

3. FIȘĂ DE CAZ – Prelucrarea nelegală a datelor cu caracter personal prin intermediul unui site aparținând unei persoane fizice

Mai multe persoane fizice au sesizat Autoritatea națională de supraveghere cu privire la o posibilă încălcare a dispozițiilor Regulamentul (UE) 2016/679, referitoare la prelucrarea datelor cu caracter personal prin intermediul unui site, pe care putea fi generată declarația pe propria răspundere necesară deplasării în afara locuinței pe perioada stării de urgență, declarată din anul 2020, în scopul prevenirii și combaterii pandemiei de COVID – 19.

În fapt, ca urmare a completării datelor cu caracter personal (nume, prenume, prenume părinți, domiciliu, CNP, serie și nr. act de identitate, adresa locuinței în fapt, locul

deplasării, scopul deplasării și semnătura), site-ul în cauză genera un formular de declarație pe proprie răspundere.

La data efectuării investigației de către Autoritatea națională de supraveghere, operatorul, persoană fizică, nu a putut prezenta dovezi din care să rezulte că a prelucrat în mod legal datele cu caracter personal, colectate și stocate pe site, nu a prezentat dovezi din care să rezulte că a asigurat informarea persoanelor vizate în legătură cu prelucrarea datelor lor personale, colectate prin intermediul site-ului și nu a efectuat configurările necesare împotriva accesării neautorizate prin intermediul internetului.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 974.89 lei (echivalentul a 200 EURO), pentru încălcarea dispozițiilor art. 5 alin. (1) lit. a) și b) și alin. (2), art. 13 alin. (1) - (3) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

4. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal pe rețelele de socializare

Un operator din domeniul bancar a notificat Autoritatea națională de supraveghere cu privire la producerea unor incidente de încălcare a securității datelor cu caracter personal, prin completarea formularului aprobat prin Decizia nr. 128/2018.

Încălcarea securității datelor cu caracter personal s-a produs ca urmare a faptului că un angajat din call center-ul persoanei împuternicite de operator a atașat, dintr-o eroare, la e-mailul transmis către un client al operatorului, un fișier excel conținând datele clienților respectivului operator care utilizau serviciul de Internet Banking.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat, raportat la prevederile art. 29 și art. 32 din Regulamentul (UE) 2016/679, că persoana împuternicită de operator nu a luat măsuri adecvate pentru a se asigura că orice persoană fizică care acționează sub autoritatea sa și care are acces la date cu caracter personal nu le prelucrează decât la cererea sa. Această încălcare a condus la divulgarea neautorizată sau accesul neautorizat la anumite date cu caracter personal, cum ar fi adresa de e-mail, nume de utilizator, CNP utilizator, număr de telefon, numele clientului, codul clientului, PIN-ul clientului, fiind afectate de incident un număr de 11.169 persoane fizice vizate.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 9.898,00 lei (echivalentul a 2000 EURO), pentru încălcarea art. 29, art. 32 alin. (1) lit. b) și art. 32 alin. (4) din Regulamentul (UE) 2016/679.

E. Investigații în alte cazuri

Încălcările de securitate a datelor cu caracter personal notificate de către entitățile din domeniul privat au avut ca obiect, în principal, nerespectarea prevederilor art. 32 din Regulamentul (UE) 2016/679 și au fost generate de neimplementarea de măsuri tehnice și organizatorice adecvate, ceea ce a condus la divulgarea sau accesul neautorizat la datele cu caracter personal prelucrate, precum și de faptul că operatorul nu a luat măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la datele cu caracter personal nu le prelucrează decât la cererea operatorului.

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

În majoritatea cazurilor, operatorii investigați au îndeplinit măsurile de remediere dispuse, în termenul acordat de Autoritatea națională de supraveghere.

1. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal către destinatari eronați și divulgarea neatorizată după retragerea consimțământului persoanelor vizate

O societate comercială a notificat Autoritatea națională de supraveghere cu privire la producerea unui număr de 24 de incidente de încălcare a securității datelor cu caracter personal, în perioada 17 iulie 2020 – 28 septembrie 2021, prin completarea formularului aprobat prin Decizia nr. 128/2018.

În fapt, încălcările de securitate notificate au avut ca obiect: publicarea datelor cu caracter personal ale unor persoane cu funcții de decizie din cadrul societății, în Sistemul Electronic de Achiziții Publice (SEAP), pe site-ul www.e-licitatie.ro, dezvăluirea datelor cu caracter personal ale unor angajați ai companiei, printr-un e-mail transmis către un grup de comunicare intern, la care s-a atașat în mod eronat un document de lucru excel, contactarea

telefonică a unei persoane vizate în vederea finalizării contractului de energie electrică, după ce aceasta renunțase la contract și își retrăsese consimțământul de prelucrare a datelor sale printr-o cerere de ștergere de date, transmiterea din eroare a unui e-mail ce conținea contractul de energie electrică și notificarea aferentă pentru schimbarea furnizorului de energie electrică, către alt destinatar, transmiterea din eroare, către un alt destinatar a unui e-mail ce conținea documente (cererea de încheiere a contractului de furnizare, copia cărții de identitate, contractul de furnizare al energiei electrice și copia ultimei facturi emise de furnizorul actual) care aparțineau și erau adresate unei alte persoane fizice, stocarea în mod neautorizat pe o partiție cu acces limitat, a datelor unei persoane vizate și încheierea contractului de energie electrică cu persoana vizată, ulterior admiterii și confirmării cererii acesteia de ștergere a datelor sale cu caracter personal, prelucrarea nelegală a datelor cu caracter personal ale unui potențial client, ulterior confirmării ștergerii acestora, prin transmiterea unui e-mail automat referitor la modificarea perioadei pentru preluarea autocitirilor și transmiterea, în mod accidental, către un alt destinatar, a unui e-mail ce conținea contractul de furnizare energie electrică al unui alt client.

Autoritatea națională de supraveghere a efectuat o investigație și a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prezentat de prelucrare, generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată au accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod, incluzând capacitatea de a asigura confidențialitatea. Aceasta a condus la accesarea ori divulgarea ilicită către destinatari eronați, a datelor cu caracter personal (nume, prenume, domiciliu, serie si număr act de identitate, cod numeric personal, număr de telefon, adresa de domiciliu, telefonul de contact, data nașterii, locul nașterii, funcția, codul unic loc de consum, informații din ultima factură emisă de furnizorul de energie actual, informații privind locurile de consum, consum estimat, semnătură, date cu privire la proprietate sau declarație pe propria răspundere), ale clienților proprii (325 persoane vizate).

Totodată, s-a constatat că operatorul investigat a prelucrat datele cu caracter personal ale clienților proprii (3 persoane vizate) după ce aceștia și-au exercitat dreptul la ștergerea datelor și și-au retras consimțământul pentru prelucrarea datelor, fără existența unui temei legal prevăzut de art. 6 alin. (1) din Regulamentul (UE) 2016/679. Potrivit art. 5 alin. (1) lit.

a) din Regulamentul (UE) 2016/679, operatorul avea obligația de a prelucra datele în mod legal, echitabil și transparent față de persoanele vizate.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 24.739,50 lei (echivalentul a 5000 EURO), pentru încălcarea art. 32 alin. (1) lit. b) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

În același timp, operatorul a fost sancționat cu avertisment pentru încălcarea art. 5 alin. (1) lit. a) și art. 6 alin. (1) din Regulamentul (UE) 2016/679.

De asemenea, în temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 16 alin. (5) din Legea nr. 102/2005, s-au dispus și următoarele măsuri corective:

a) Revizuirea și actualizarea măsurilor tehnice și organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal, precum și implementarea unor măsuri privind instruirea periodică a persoanelor care acționează sub autoritatea sa, referitor la obligațiile ce le revin conform prevederilor Regulamentului (UE) 2016/679, inclusiv cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcţie de specificul activităţii.

b) Identificarea și implementarea unor măsuri pentru a se asigura că datele cu caracter personal prelucrate sunt exacte și actualizate, având în vedere scopurile pentru care sunt prelucrate, inclusiv în ceea ce privește evidența exercitării dreptului la ștergerea datelor cu caracter personal, de către persoanele vizate.

2. FIȘĂ DE CAZ – Dezvăluirea neautorizată a datelor cu caracter personal prelucrate de către un magazin on-line

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, documente de transport, care însoțesc expedierea coletelor, pentru identificarea unică și urmărirea acestora, precum și documente care conțin date cu caracter personal ale clienților unui magazin on-line, sunt disponibile publicului pe un site, prin accesarea unui link. Datele cu caracter personal divulgate pe site sunt: nume și prenume, numere de telefon, adrese de reședință și adrese ale unor locuri de muncă.

Autoritatea națională de supraveghere a efectuat o investigație și a constatat că societatea care deținea site-ul pe care erau divulgate datele cu caracter personal nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării pentru drepturile și libertățile persoanelor fizice, generat în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod sau accesul neautorizat la acestea. Aceasta a condus la divulgarea și accesul neautorizate la datele cu caracter personal prin accesarea unui link, unde erau disponibile public informații cu privire la documentele de transport care însoțesc expedierea coletelor, care conțin date cu caracter personal ale persoanelor fizice, clienți ai magazinului on-line, cum ar fi: nume și prenume, numere de telefon, adrese de reședință și adrese locuri de muncă, deși potrivit art. 5 lit. f) din Regulamentul (UE) 2016/679, operatorul avea obligația de a respecta principiul "integritate și confidențialitate".

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de e 9.769,2 lei (echivalentul a 2000 EURO), pentru încălcarea art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679, în temeiul art. 58 alin. (2) lit. i) din Regulamentul (UE) 2016/679.

3. FIȘĂ DE CAZ – Prelucrarea datelor cu caracter personal ale angajaților în scopul realizării accesului și pontajului angajaților proprii

Autoritatea națională de supraveghere a fost sesizată cu privire la prelucrarea datelor biometrice (amprentă) de către o regie autonomă, în scopul realizării accesului și pontajului angajaților.

Urmare a investigației efectuate la nivelul operatorului, acesta a declarat drept scop principal al prelucrării datelor biometrice, creșterea nivelului de securitate în locațiile critice ale instituției, crearea unui loc de muncă mai sigur, prin verificarea accesului angajaților ca parte din procesul de control al permisiunilor, respectiv simplificarea și eficientizarea modului în care este administrată prezența angajaților.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul a prelucrat datele biometrice (amprente) ale aproximativ 500 de angajați, reprezentând 1/3 din numărul total al acestora, date considerate a nu fi adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate

("reducerea la minimum a datelor") în cadrul procesului de testare a sistemului bazat pe date biometrice, scopul declarat de operator (accesul/pontajul angajaților) putându-se realiza prin mijloace mai puțin intruzive pentru viața privată a angajaților.

De asemenea, Autoritatea națională de supraveghere a constatat că datele biometrice (amprentele digitale) colectate de la aproximativ 500 de angajați și utilizate în vederea testării sistemului de control acces/pontaj nu sunt colectate în scopuri adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor"), putându-se realiza prin mijloace mai puțin intruzive pentru viața privată a angajaților. În acest sens s-au avut în vedere declarațiile operatorului potrivit cărora, la momentul investigației, pontajul și accesul angajaților se realiza exclusiv prin intermediul cartelelor de acces (procedura standard anterioară introducerii metodei bazate pe date biometrice).

Temeiurile legale invocate de către operator nu au fost reținute deoarece operatorul nu a făcut dovada necesității prelucrării datelor biometrice (amprentă) în scopul îndeplinirii obligațiilor specifice și exercitarea unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale și nici a faptului că utilizarea metodei biometrice pentru pontaj/control acces este autorizată de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate, și nici că prelucrarea acestor date este necesară.

Autoritatea națională de supraveghere a sancționat operatorul cu avertisment, pentru încălcarea prevederilor art. 5 alin. (1) lit. c) din Regulamentul (UE) 2016/679, prin raportare la condițiile privind legalitatea prelucrării stabilite de art. 9 din Regulamentul (UE) 2016/679.

4. FIȘĂ DE CAZ – Prelucrarea neautorizată a datelor cu caracter personal ale angajaților prin intermediul sistemului de supraveghere video

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o societate comercială are instalate camere de supraveghere audio-video în interiorul birourilor, pentru supravegherea directă a angajaților la locul de muncă unde își desfășoară activitatea și înregistrarea discuțiilor dintre aceștia, în scopul utilizării lor ulterioare împotriva respectivilor angajați.

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că operatorul a prelucrat date cu caracter personal ale angajaților săi prin utilizarea unui sistem audio-video, fără a face dovada respectării temeiurilor legale prevăzute de art. 6 alin. (1) din Regulamentul (UE) 2016/679, respectiv obținerea consimțământului persoanelor vizate, îndeplinirea unei obligații legale sau prevalența interesului său legitim asupra intereselor, drepturilor și libertăților persoanelor vizate.

De asemenea, Autoritatea națională de supraveghere a constatat faptul că operatorul a luat măsura monitorizării angajaților la locul de muncă prin sisteme de supraveghere audio-video fără a respecta principiul prevăzut de art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679, potrivit căruia operatorul are obligația de a prelucra datele în mod legal, echitabil și transparent față de persoana vizată.

Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 24.745,00 lei (echivalentul a 5000 EURO), pentru încălcarea prevederilor art. 5 alin. (1) lit. a) raportat la art. 6 alin. (1) din Regulamentul (UE) 2016/679.

În temeiul art. 58 alin. (2) lit. d) din Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere a dispus și măsura corectivă de a se asigura conformitatea operațiunilor de prelucrare efectuate prin utilizarea sistemelor audio-video, precum și încetarea oricărei operațiuni sau set de operațiuni de prelucrare de date cu caracter personal efectuate prin intermediul sistemelor audio-video și ștergerea sistemului de evidență a datelor cu caracter personal constituit ca urmare a utilizării unor astfel de sisteme.

Operatorul a contestat în instanță sancțiunea aplicată, dosarul fiind pe rolul instanțelor de judecată.

Secţiunea a 3 - a: Activitatea de soluţionare a plângerilor

1. Prezentare generală

În anul 2021, 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 **4634 plângeri**, care au vizat, în principal, următoarele aspecte:

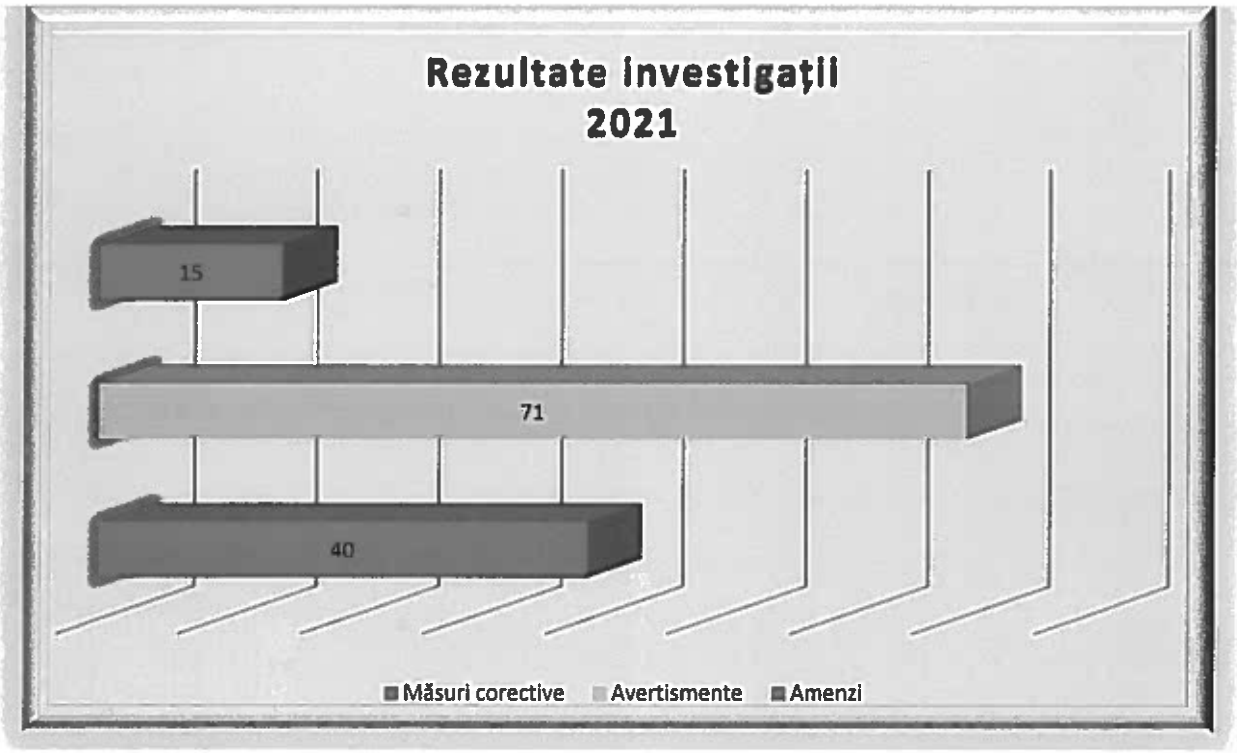
- încălcarea drepturilor persoanelor vizate, în special a dreptului de acces al persoanei vizate, de opoziție și a dreptului la ștergerea datelor;
- prelucrarea imaginilor prin intermediul sistemelor de supraveghere video instalate de anagajatori la locul de muncă sau de asociațiile de proprietari în condominii;
- dezvăluirea datelor personale pe internet, inclusiv pe rețelele de socializare;
- prelucrarea datelor personale cu încălcarea prevederilor art. 6 din Regulamentul (UE) 2016/679 privind stabilirea corectă a temeiului legal ori lipsa acestuia;
- încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date cu caracter personal;
- primirea de mesaje comerciale nesolicitate prin telefon sau poștă electronică.

Pentru soluționarea plângerilor considerate admisibile au fost demarate **319 investigații**.

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

- **15 amenzi**, dintre care **14 amenzi** în baza Regulamentului (UE) 2016/679, reprezentând un cuantum total de **141.530,1 Lei** (echivalentul sumei de **28.700 Euro**) și **o amendă** în baza Legii nr. 506/2004, modificată și completată, în cuantum total de **10.000 Lei**;

- **71 de avertismente;**
- **40 măsuri corective** în baza dispozițiilor art. 58 alin. (2) lit. c) și d) din Regulamentul (UE) 2016/679.



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

- asigurarea conformității operațiunilor de prelucrare cu dispozițiile Regulamentului (UE) 2016/679;
- respectarea principiilor de prelucrare a datelor, în special cele privind legalitatea, transparența și proporționalitatea;
- respectarea drepturilor persoanelor vizate prevăzute de Regulamentul (UE) 2016/679;
- realizarea informării persoanelor vizate potrivit art. 12 din Regulamentul (UE) 2016/679, inclusiv prin utilizarea de pictograme standardizate în spațiile/locurile monitorizate video, poziționate la o distanță rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere;
- implementarea de măsuri tehnice și organizatorice adecvate pentru asigurarea securității și confidențialității datelor, precum și respectarea acestor măsuri.

2. Principalele constatări rezultate din activitatea de soluționare a plângerilor

A. Dezvăluirea datelor personale către diverse entități

În anul 2021, prin multe dintre plângerile adresate Autorității naţionale de supraveghere, petenții au semnalat încălcări ale dispozițiilor legale de către operatori, ca urmare a dezvăluirii datelor lor (ex. inclusiv a unor categorii speciale de date, precum datele privind starea de sănătate) fie către publicul larg (ex. presă, posturi de televiziune), fie către entități de drept public sau privat sau către terțe persoane neautorizate, fără să fi fost obţinut în prealabil acordul persoanelor vizate sau fără să existe un alt temei legal.

1. FIȘĂ DE CAZ

Un petent, angajat al unui spital județean, a reclamat faptul că managerul interimar al acestui spital a dat publicității, cu ocazia unor emisiuni de televiziune, o serie de aspecte cu privire la desfășurarea unor studii clinice în care au fost implicați pacienți cu afecțiuni psihiatrice din acest spital, ce ar fi fost coordonate de petent (medic psihiatru). Astfel, s-a reclamat faptul că au fost dezvăluite ilegal numele său și datele unor terțe persoane (pacienți, prestatori de servicii).

În cadrul investigației efectuate în acest caz, s-a constatat că, prin modul de manipulare a unor înscrisuri în fața camerelor de filmare de la posturile de televiziune respective, cu ocazia interviului acordat acestora de către managerul spitalului, a fost posibilă filmarea unor documente ce conțineau în mod vizibil date personale. Cu toate că operatorul investigat a declarat că divulgarea a fost una accidentală, nu a precizat care a fost temeiul legal și care au fost motivele pentru care au fost folosite de această manieră documente conținând datele personale, acordarea interviului fiind posibilă fără dezvăluirea acestor date, în circumstanțele descrise.

Față de cele constatate, s-a dispus aplicarea unui avertisment, pentru încălcarea art. 6 și 9, prin raportare la principiile prevăzute de art. 5 alin. (1) lit. a), b), c) și f) și alin. (2) din RGPD.

Totodată, prin planul de remediere, s-a dispus instruirea regulată a persoanelor care prelucrează date personale sub autoritatea operatorului, cu privire la necesitatea respectării prevederilor RGPD, inclusiv în cazul relațiilor cu presa.

2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de o petentă cu privire la dezvăluirea datelor sale de sănătate de către o policlinică, unde fusese în trecut pacientă și angajată, în cadrul unor dosare civile aflate pe rolul instanțelor de judecată.

Ca urmare a investigației efectuate în acest caz, s-a constatat că datele personale și de sănătate ce o privesc pe petentă au fost dezvăluite de policlinică către avocatul uneia dintre părți, în scopul de a fi folosite în două dosare civile de pe rolul instanțelor de judecată, unde unii dintre membrii de familie ai părților aveau calitatea de martor sau au fost propuși ca martori, fiind totodată asociați la această policlinică, fără să fie dovedită obligativitatea prezentării unor astfel de date și documente în baza dispozițiilor instanței de judecată. Policlinica nu a prezentat dovezi privind informarea prealabilă a petentei, înainte de dezvăluirea datelor sale.

Față de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 9898 lei (echivalentul a 2.000 euro), pentru încălcarea art. 5 alin. (1) lit. a), b) și f) și alin. (2) din RGPD, coroborate cu art. 9 din RGPD.

Totodată, s-a dispus aplicarea unei măsuri corective de a asigura conformitatea cu RGPD a operațiunilor de colectare și prelucrare ulterioară a datelor personale, asfel încât să se evite dezvăluirea datelor personale prelucrate, cu încălcarea condițiilor legale.

În acest sens, s-a dispus aplicarea unor măsuri adecvate de securitate și confidențialitate, prin instruirea regulată a persoanelor care prelucrează date sub autoritatea operatorului și implicarea corespunzătoare a responsabilului cu protecția datelor personale potrivit art. 37-39 din RGPD.

3. FIȘĂ DE CAZ

Un petent a sesizat o posibilă încălcare a Regulamentului (UE) 2016/679 de către o instituție de învățământ superior care i-ar fi dezvăluit datele personale, în condițiile în care o cerere, adresată de el acestei instituții a ajuns, în integralitatea ei, inclusiv cu adresa sa de domiciliu neanonimizată, în posesia unei publicații care a postat-o în cadrul unui articol.

În cursul investigaţiei, operatorul a declarat că, urmare a primirii unei cereri în baza Legii nr. 544/2001 privind liberul acces la informațiile de interes public, modificată şi completată, din partea unei publicații electronice, prin care se solicitau informații referitoare la petent, care avea calitatea de persoană publică, a fost transmis un răspuns, la care a atașat cererea pe care i-o adresase petentul, în integralitatea sa.

Legea nr. 544/2001, modificată şi completată, prevede, la art. 12 alin. (1) lit. d), că se exceptează de la accesul liber al cetăţenilor informaţiile cu privire la datele cu caracter personal, potrivit legii. Totodată, potrivit art. 14 alin. (1) din Legea nr. 544/2001, modificată și completată, informaţiile deţinute de către o autoritate sau instituţie publică cu privire la datele personale ale unui cetăţean pot deveni informaţii de interes public numai în măsura în care afectează capacitatea de exercitare a unei funcţii publice.

Corelat, RGPD stabileşte condiţiile în care datele cu caracter personal pot fi prelucrate (inclusiv dezvăluite către terți, comunicate, utilizate, etc.).

Astfel, pentru transmiterea documentelor referitoare la petent către un terț, instituția de învățământ superior, în calitate de operator, trebuia să respecte prevederile RGPD, în special art. 5 și art. 6 din RGPD.

Întrucât această cerere cuprindea datele cu caracter personal ale petentului, inclusiv adresa de domiciu și semnătura, prin transmiterea acesteia unei publicații fără anonimizarea datelor personale, instituția de învățământ superior a încălcat prevederile art. 5 din RGPD, care reglementează principiile legate de prelucrarea datelor cu caracter personal, conform cărora datele personale trebuie prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată ("legalitate, echitate şi transparenţă").

De asemenea, operatorul nu a prezentat dovezi că dezvăluirea datelor cu caracter personal ale petentului, respectiv adresa și semnătura, a fost efectuată cu consimțământul acestuia sau în baza altui temei legal reglementat la art. 6 din RGPD.

În consecință, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea art. 5 alin. (1) lit. a) și art. 6 din RGPD și i s-a stabilit obligația de a implementa măsuri pentru ca dezvăluirea datelor către terți să fie efectuată cu respectarea acestor prevederi.

B. Încălcarea principiilor de prelucrare a datelor

În cadrul multora dintre investigațiile efectuate pentru soluționarea plângerilor adresate Autorității naționale de supraveghere, s-a verificat inclusiv respectarea principiilor de prelucrare a datelor personale, prevăzute de art. 5 din RGPD.

Astfel, s-a constatat că unii operatori nu prelucrează datele personale în mod transparent și echitabil față de persoanele vizate ori colectează date care nu sunt adecvate și relevante prin raportare la scopurile prelucrării datelor. În alte cazuri, s-a observat că datele personale supuse prelucrării nu erau exacte și actualizate, fapt de natură a produce prejudicii persoanelor vizate.

În toate aceste situații, operatorii au încălcat inclusiv principiul responsabilității, conform căruia sunt obligați să asigure și să demonstreze respectarea tuturor celorlalte principii reglementate de art. 5 alin. (1) din RGPD.

În funcție de circumstanțele fiecărui caz, Autoritatea națională de supraveghere a aplicat sancțiuni contravenționale (avertisment sau amendă) și a dispus corectarea practicilor nelegale printr-o serie de măsuri emise în temeiul art. 58 alin. (2) din RGPD.

Prezentăm mai jos câteva cazuri relevante.

1. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o instituție financiar-bancară cu care petentul avea încheiat un contract de credit în numele societății pe care o reprezenta, i-a utilizat fără acord datele personale, în cadrul unor proceduri de executare silită pentru debitele rezultate dintr-un contract de credit de care nu avea cunoștință, aspect de care a aflat cu ocazia primirii unor notificări din partea unor executori judecătorești. Petentul a solicitat băncii să-i comunice "toate actele care stau la baza calculării debitului", iar ulterior a solicitat și să revoce cele două notificări, să remedieze eroarea materială și să înceteze utilizarea datelor personale în alte scopuri decât cele pentru care le-

a încredințat băncii. Petentul a susținut că nu a primit răspuns la niciuna din cele patru cereri adresate băncii.

Petentul reclama, așadar, folosirea fără consimțământ a datelor sale personale, în alte scopuri decât cele autorizate de dumnealui, utilizarea unei adrese care nu mai este de actualitate și pentru care petentul considera că banca a accesat ilegal o bază de date, lipsa informării cu privire la sursa de colectare a acestor informații conform art. 14 din RGPD, precum și lipsa răspunsului la cererile adresate către bancă.

În cadrul investigației efectuate în acest caz, s-a constatat că, dintr-o eroare a unui angajat al băncii, datele petentului au fost introduse în baza de date și atribuite acestuia (în calitate de fidejusor), asociate la datele unei alte societăți cu care petentul nu avea niciun fel de legătură, iar ulterior, în cadrul procedurii de notificare privind restanțele acumulate de această societate, datele sale au fost dezvăluite inclusiv către executorul judecătoresc. În cadrul acestei proceduri de notificare au fost folosite adresele de domiciliu ale petentului, existente în baza de date a băncii, prima fiind colectată cu ocazia unei tranzacții anterioare efectuate de petent în nume propriu; cu toate că prima adresă era marcată în sistemul informatic ca fiind expirată, dintr-o eroare, angajatul băncii a folosit-o în transmiterea uneia dintre cele două notificări expediate prin intermediul executorului judecătoresc. Reprezentanții băncii au declarat că s-a remediat eroarea legată de asocierea datelor petentului cu o altă societate și a fost îmbunătățit procesul de notificare, prin extragerea automată din sistemul informatic a adreselor de contact actualizate. De asemenea, au fost prezentate dovezi cu privire la transmiterea în termen legal a răspunsurilor la cererile depuse de petent, aceste aspecte nefiind așadar confirmate.

Față de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 9.855,8 lei (echivalentul a 2.000 euro), pentru încălcarea art. 5 alin. (1) lit. a) și d) și alin. (2) și a art. 6 din RGPD.

Totodată, s-a dispus aplicarea unei măsuri corective de a asigura conformitatea cu RGPD a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin implementarea unor metode eficiente de respectare a caracterului exact și actual al datelor, de la momentul colectării datelor și introducerii lor în baza de date a operatorului și pe întreaga perioadă de prelucrare; în acest sens, s-a dispus punerea în practică a unor măsuri adecvate și eficiente de securitate, atât din punct de vedere tehnic sub aspectul ștergerii

datelor inexacte/care nu mai sunt de actualitate, cât și din punct de vedere organizatoric, prin instruirea regulată a persoanelor ce prelucrează date sub autoritatea operatorului.

2. FIȘĂ DE CAZ

Un petent a reclamat primirea pe adresa sa de e-mail a unor facturi și mesaje de notificare cu privire la restanțele acumulate de o altă persoană, abonat al unui furnizor de servicii de telefonie. Cu toate că petentul a adus la cunoștința acestei companii și a societății împuternicite pentru recuperarea creanțelor eroarea cu privire la prelucrarea adresei sale de e-mail în repetate rânduri, iar cele două societăți i-au confirmat remedierea acesteia, a continuat să primească pe adresa sa mesaje referitoare la abonatul respectiv.

În cadrul investigației efectuate în acest caz, s-a constatat că adresa de e-mail a petentului, scrisă cu litere mici, a fost asociată pentru un cont al furnizorului, într-o "presupusă" acțiune de actualizare a datelor de contact pe cont, iar aceeași adresă, dar scrisă cu majuscule, a fost asociată contului altui client la o dată ulterioară, ca urmare a declarării de către client ca adresă de corespondență electronică pentru transmiterea facturii, la momentul încheierii contractului. Cu toate acestea, nu era clar dacă în ambele situații cele două adrese au fost declarate ca atare de persoanele respective sau au fost incluse în baza de date în mod eronat de către angajații/colaboratorii operatorului, prin modalitatea de tehnoredactare a acestor adrese de e-mail. De altfel, din anexele la plângere rezulta că aceste două adrese de e-mail nu sunt diferite, deși scrise cu litere mari sau mici. Urmare a reclamației petentului, operatorul a confirmat ștergerea adresei de e-mail scrisă cu litere mici, însă, din cauza unei erori a funcției de căutare, nu a fost ștearsă și adresa scrisă cu majuscule. Ca atare, din acest motiv, petentul a continuat să primească pe adresa sa de e-mail diverse notificări de plată a facturilor și mesaje electronice adresate unei alte persoane, din partea operatorului și a persoanei împuternicite pentru recuperarea debitelor restante.

Față de cele constatate, având în vedere că operatorul în cauză nu se afla la prima abatere constatată de Autoritatea națională de supraveghere, s-a dispus aplicarea a două amenzi în cuantum de 24.745 lei (echivalentul a 5.000 euro), respectiv, de 4.949 lei (echivalentul a 1.000 euro), pentru încălcarea art. 5 alin. (1) lit. d) și f), art. 5 alin. (2) din RGPD, respectiv, a art. 17 din RGPD.

De asemenea, s-au aplicat două măsuri corective, respectiv cea de a asigura conformitatea cu RGPD a operațiunilor de colectare și prelucrare ulterioară a datelor

personale, prin implementarea unor metode eficiente de asigurare a exactității datelor, cât și în cazul soluționării cererilor de ștergere sau rectificare a datelor personale, prin adoptarea unor măsuri tehnice și organizatorice adecvate care să garanteze implementarea efectivă și corectă a acestor operațiuni în baza/bazele de date folosite de operator și persoanele împuternicite de acesta, precum și cea privind instruirea corespunzătoare a persoanelor care prelucrează date sub autoritatea acestora.

C. Nerespectarea drepturilor de informare, acces, intervenție și opoziție

În anul 2021, nerespectarea drepturilor persoanelor vizate a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere. Astfel, ca urmare a investigațiilor efectuate, s-a constatat faptul că unii operatori de date cu caracter personal nu au soluționat cererile adresate de persoanele vizate (în special referitor la dreptul de acces și dreptul de ștergere), în exercitarea drepturilor lor sau nu au respectat termenul în care trebuie să furnizeze persoanelor vizate informații privind acțiunile întreprinse în urma depunerii unei cereri în temeiul art. 15-22 din Regulamentul (UE) 2016/679, precum și faptul că nu au stabilit modalități concrete de exercitare a drepturilor persoanelor vizate.

1. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de un petent cu privire la faptul că un operator i-a încălcat dreptul de ștergere.

Petentul a susținut că a solicitat prin intermediul poștei electronice ștergerea tuturor datelor referitoare la contul înregistrat pe platforma societății, dar nu a primit un răspuns. Solicitarea a fost transmisă către adresa de e-mail a responsabilului cu protecția datelor cu caracter personal al societății reclamate.

Ca urmare a investigației efectuate, s-a constatat că operatorul nu a soluționat cererea petentului privind ștergerea tuturor datelor referitoare la contul înregistrat în termenul prevăzut de art. 12 alin. (3), fiind transmis un răspuns petentului ulterior termenului stabilit în articolul menționat mai sus.

Față de aceste constatări, operatorul a fost sancționat contravențional cu avertisment. De asemenea, s-a recomandat operatorului să ia măsuri astfel încât să fie respectate, în toate cazurile, prevederile art. 12 din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ

O petentă a sesizat Autoritatea națională de supraveghere în legătură cu o posibilă încălcare a legislației privind protecția datelor personale de către o societate comercială, deoarece la cererile prin care și-a exercitat dreptul de acces la propriile date, respectiv la imaginea sa preluată prin intermediul sistemului de supraveghere instalat în unul dintre magazinele operatorului, a primit doar o parte dintre aceste date.

Ca urmare a investigației efectuate, a reieșit că operatorul nu a comunicat, la cererile petentei, toate informațiile solicitate, cu toate că aceasta furnizase suficiente detalii pentru a permite identificarea imaginilor cerute: locul supus monitorizării, data înregistrării și intervalul orar, inclusiv elementele necesare pentru identificarea sa prin transmiterea unei copii a actului de identitate (în care puteau fi vizualizate doar numele și prenumele și poza).

În plus, s-a constatat că la data depunerii cererii de către petentă, prin care a solicitat acces la datele sale, acestea erau încă disponibile, neexpirând termenul de stocare a acestora.

Având în vedere prevederile art. 15 din RGPD, comunicarea unei înregistrări video ce conține date (imagini) care privesc persoana vizată, ca urmare a exercitării dreptului de acces de către aceasta, reprezintă o obligație a operatorului, comunicarea imaginilor efectuându-se de operator prin luarea măsurilor de obturare ("blurare") a acelor date care ar putea să aducă atingere drepturilor și libertăților altor persoane fizice, dacă este cazul. Prin urmare, operatorul era 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.

În acest context, operatorul de date a fost sancționat cu amendă în cuantum de 14846,4 lei, (echivalentul a 3.000 euro) pentru încălcarea prevederilor art. 15 alin. (3) din RGPD și i s-a aplicat măsura corectivă de a comunica petentei toate imaginile solicitate de aceasta, în măsura în care mai sunt disponibile, cu blurarea imaginilor care duc la identificarea altor persoane.

3. FIȘĂ DE CAZ

În anul 2021 a fost finalizată investigația începută pentru soluționarea plângerii depuse de o petentă la autoritatea pentru protecția datelor personale din Polonia, împotriva

unui operator român, fapt pentru care în această speță Autoritatea națională de supraveghere a efectuat investigația și a soluționat plângerea printr-o decizie în calitate de autoritate de supraveghere principală, în baza competențelor prevăzute de mecanismele de cooperare din RGPD și de Legea nr. 102/2005.

Petenta a reclamat faptul că datele sale personale (nume, prenume, profesie, adresă, aferente unei forme de organizare juridică care nu mai era valabilă) erau publicate, printre altele, pe site-ul deținut de o societate cu sediul în România (site disponibil în diverse versiuni de nume de domenii europene și în limbile naționale ale statelor membre ale UE, precum: română, franceză, italiană, finlandeză, spaniolă, germană, slovacă, suedeză, maghiară, poloneză, cehă, daneză, olandeză). Petenta s-a adresat pe e-mail invocând art. 17 și 21 din RGPD pentru a obține ștergerea acestor date publicate fără acordul și informarea sa, cererea sa nefiind soluționată până la data depunerii plângerii.

În cadrul investigației efectuate în acest caz, s-a constatat că operatorul din România a colectat datele personale ale petentei în calitatea acesteia de profesionist din baze de date publice disponibile în Polonia. Dintr-o eroare, solicitarea petentei nu a fost procesată în mod corespunzător, întrucât e-mail-ul său a intrat în spam, iar operatorul a omis deschiderea și procesarea e-mail-ului, cu toate că, de obicei, astfel de cereri se procesează în termene foarte scurte.

În consecință, operatorul, aflând de solicitarea petentei abia în urma primirii adresei Autorității naționale de supraveghere, a șters fără întârziere toate datele aparținând profesionistului, a luat măsuri ca toate e-mail-urile să fie citite și procesate cu rigurozitate maximă și a adus la cunoștința petentei măsurile adoptate pe e-mail.

Față de cele constatate și luând în considerare obiecțiile relevante și motivate formulate de unele autorități de supraveghere vizate, a fost emisă o decizie prin care s-au aplicat două sancțiuni contravenționale (avertismente) pentru încălcarea art. 17 și respectiv, art. 12-14 din RGPD.

De asemenea, s-au dispus două măsuri corective, prin care operatorului i s-au pus în vedere următoarele:

- să pună în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea datelor se efectuează în conformitate cu RGPD, inclusiv prin punerea în aplicare de către operator a unor politici adecvate de protecţie a datelor, ce trebuie să includă măsuri adecvate și eficiente pentru ca orice cerere primită la

datele de contact publice indicate, din partea persoanelor care doresc să își exercite drepturile prevăzute de RGPD, să fie analizată și soluționată în condițiile și termenele prevăzute de art. 12-22 din RGPD;

- să asigure legalitatea prelucrării datelor persoanelor fizice ale căror date personale sunt disponibile prin intermediul cataloagelor on line, conform art. 5 și 6 din RGPD și să furnizeze informații complete, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, potrivit art. 12-14 din RGPD, cu privire la prelucrarea datelor acestor persoane, respectiv să respecte drepturile acestor persoane, așa cum sunt acestea prevăzute de art. 15-22 din RGPD, facilitând, totodată, exercitarea lor; în acest sens, s-a dispus completarea în mod corespunzător a informării existente pe fiecare versiune lingvistică a site-urilor aparținând operatorului, pe care sunt puse la dispoziția publicului cataloage on-line.

Această decizie face obiectul publicării în registrul ținut pe site-ul Comitetului European pentru Protecția Datelor.

4. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la primirea unor apeluri telefonice nesolicitate în scopuri de marketing, în cadrul cărora petentului i s-a cerut să confirme numele său. Ulterior, petentul s-a adresat pe e-mail către societatea respectivă, cu solicitarea de a-i fi șterse orice date personale ar deține, inclusiv adresa de e-mail și numele asociat contului de facebook de pe care încercase să contacteze societatea, comunicând totodată că se opune prelucrării datelor sale, întrucât societatea nu deține consimțământul său în acest sens. Mesajele trimise către cele două adrese de e-mail ale societății (indicate pe site-ul acesteia, una aparținând responsabilului cu protecția datelor) au fost returnate, petentul neprimind niciun răspuns la cererea sa.

Aspectele reclamate au făcut obiectul unei investigații, însă, cu toate că adresele Autorității naționale de supraveghere au fost trimise în mod repetat către datele de contact publice ale societății (inclusiv prin intermediul executorului judecătoresc), operatorul nu a dat curs solicitărilor adresate. Adresele de investigație au fost transmise inclusiv către adresa de poștă electronică furnizată pe site-ul operatorului ca dată de contact a responsabilului cu protecția datelor (folosită și de petent).

Prin urmare, inclusiv solicitările trimise către datele de contact indicate pe site-ul operatorului în scopul transmiterii cererilor pentru exercitarea drepturilor de către persoanele vizate (cum a fost și cazul petentului) nu erau gestionate în scopul soluționării lor, deși operatorul este obligat să adopte măsuri prin care să faciliteze efectiv exercitarea drepturilor persoanelor vizate.

Față de cele constatate, s-a dispus aplicarea unei amenzi în cuantum de 9.839,4 lei (echivalentul a 2.000 euro), pentru refuzul de a comunica Autorității naționale de supraveghere informațiile solicitate în exercitarea competențelor sale de investigare, precum și un avertisment pentru încălcarea art. 12 alin. (2) și (3) din RGPD.

De asemenea, s-au dispus două măsuri corective, prin care operatorului i s-a pus în vedere să răspundă la cererea petentului, privind măsurile adoptate referitoare la ștergerea datelor acestuia, colectate fără consimțământul său expres, precum și să faciliteze exercitarea drepturilor persoanelor vizate, prin punerea la dispoziția acestora a unor date de contact valabile, inclusiv a unei adrese de e-mail funcționale, acestea urmând a fi făcute publice pe site-ul său la secțiunile dedicate colectării datelor personale, inclusiv la secțiunile privind prelucrarea datelor personale, politica de confidențialitate, datele de contact.

5. FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că i-a fost încălcat dreptul de acces.

Petentul a susținut că a primit mesaje comerciale nesolicitate de la operator. Ulterior, s-a adresat magazinului on-line și a solicitat informații cu privire la sursa datelor sale cu caracter personal, dar nu a primit niciun răspuns.

Ca urmare a investigației efectuate s-a constatat că operatorul a încălcat dispozițiile art. 12 și 15 din Regulamentul (UE) 2016/679 întrucât nu a făcut dovada că a transmis un răspuns petentului la cererile sale prin care a solicitat informații cu privire la sursa datelor sale cu caracter personal.

Față de constatări, operatorul a fost sancționat contravențional cu avertisment și măsura corectivă de a lua măsurile necesare astfel încât să dea curs solicitărilor petentului.

De asemenea, s-a recomandat societății să ia măsurile necesare astfel încât, pe viitor, să fie respectate, în toate cazurile, drepturile persoanelor vizate prevăzute de Regulamentul (UE) 2016/679.

D. Încălcarea regulilor de confidențialitate și securitate a prelucrărilor de date

Deși implementarea unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător reprezintă una dintre principalele obligații ale operatorilor de date personale și ale persoanelor împuternicite, Autoritatea națională de supraveghere a primit o serie de plângeri, prin care era sesizată cu privire la accesarea și divulgarea neautorizată a unor date cu caracter personal către terțe persoane, ca urmare a faptului că operatorii în cauză nu au implementat proceduri interne eficiente, de ordin tehnic sau organizatoric, care să prevină apariția unor astfel de probleme.

1. FIȘĂ DE CAZ

Prin petiția adresată Autorității naționale de supraveghere, o petentă a semnalat că datele sale, cuprinse într-o petiție pe care o adresase angajatorului său, un spital, au fost dezvăluite de către un alt angajat, care a avut acces la ea în virtutea atribuțiilor de serviciu, pe un grup de WhatsApp, constituit din angajați ai acestui spital.

Petiția transmisă de petentă angajatorului său, a cărei fotografie a fost postată pe grupul de WhatsApp de către celălalt angajat, conținea numele și prenumele petentei, adresa, CNP, serie și nr. CI, adresa, telefon, funcție.

În urma investigației a reieșit că grupul de WhatsApp, alcătuit din angajați ai spitalului, a fost constituit în scopul unei comunicări eficiente și rapide a informațiilor către aceștia. Angajatorul a demarat o cercetare internă administrativă care a vizat mai multe aspecte din activitatea derulată în cadrul spitalului, fără a adopta alte măsuri cu privire la situația semnalată, respectiv fotografierea petiției petentei și postarea acesteia pe whatsapp, iar, ulterior, refuzul ștergerii postării, această operațiune fiind efectuată de către administratorul grupului de whatsapp, la solicitarea unui alt angajat.

Astfel, a rezultat că angajatorul, în cazul de față un spital, nu a adoptat suficiente măsuri de securitate pentru a asigura confidențialitatea datelor personale (numele și prenumele, adresa, CNP, serie și nr. CI, telefon, funcție, precum și informații legate de activitatea profesională) ale petentei, conform obligațiilor impuse de art. 32 din RGPD, fapt

ce a rezultat în dezvăluirea petiției petentei pe grupul de WhatsApp, permițând astfel accesul neautorizat al membrilor respectivului grup WhatsApp la datele acesteia.

În consecință, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea obligațiilor impuse de art. 32 din RGPD, care prevede, printre altele, la alin. (1) lit. b), și obligația de a implementa măsuri tehnice şi organizatorice adecvate, incluzând capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare.

Totodata, operatorului i s-a stabilit obligatia de a implementa o serie de măsuri corective, astfel încât să fie asigurată conformitatea operațiunilor de prelucrare a datelor personale cu RGPD, prin implementarea unor măsuri tehnice și organizatorice adecvate în cazul transmiterii datelor personale, inclusiv sub aspectul instruirii regulate a persoanelor care prelucrează date sub autoritatea operatorului (angajați).

2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii depuse de un petent care a sesizat faptul că o societate de transport public local a transmis răspunsul la o serie de reclamații adresate acesteia pe o adresă de e-mail aparținând altei persoane care l-a informat pe petent în legătură cu aceste aspecte.

În cadrul investigației efectuate în acest caz, s-a constatat că operatorul a dezvăluit din eroare răspunsul care trebuia trimis la petițiile petentului către o altă persoană care deținea o altă adresă de poștă electronică foarte asemănătoare cu cea a petentului, dezvăluind astfel numele și prenumele petentului, adresa sa de e-mail, precum și informații privind cererile depuse de petent și modul lor de soluționare.

Prin urmare, s-a reținut că operatorul a prelucrat date personale inexacte cu privire la petent, în scopul soluționării unei reclamații, prin redactarea greșită a adresei sale de e-mail în răspunsul formulat și prin utilizarea acesteia la expedierea răspunsului prin poșta electronică, nefiind astfel adoptate suficiente măsuri de securitate împotriva prelucrării ilegale a datelor sale personale.

Față de cele constatate, s-a dispus aplicarea unei sancțiuni contravenționale (avertisment).

De asemenea, s-au dispus măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de prelucrare a datelor personale, prin implementarea unor metode eficiente

de respectare a exactității datelor, inclusiv în cazul colectării datelor precum adresa de poștă electronică, ce permit comunicarea la distanță a datelor personale.

E. Prelucrarea datelor de către autorități publice

În cursul anului 2021, Autoritatea națională de supraveghere a primit în număr semnificativ de plângeri prin care petenții au reclamat prelucrarea datelor personale de către autorități publice. Plângerile au avut ca obiect, în principal, dezvăluirea datelor cu caracter personal pe site-urile acestor entități, încălcarea drepturilor persoanelor fizice (în special a dreptului de acces), prelucrarea imaginii prin mijloace de supraveghere video și prelucrarea fără asigurarea securității datelor.

Printre operatorii reclamați s-au numărat primării, unități de învățământ, unități medicale, structuri din cadrul poliției, autorități centrale.

În vederea soluționării plângerilor considerate admisibile, Autoritatea națională de supraveghere a efectuat o serie de investigații, în urma cărora operatorii au fost sancționați, în principal, pentru nerespectarea principiilor legate de prelucrarea datelor cu caracter personal, a condițiilor de prelucrare a datelor (legalitatea prelucrării), a drepturilor persoanelor vizate și a securității prelucrării datelor.

1. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o instituție publică a prelucrat ilegal datele cu caracter personal ale fiicei petentei, instituționalizată într-un centru de plasament aflat în subordinea respectivei autorități.

În cadrul investigației s-a constatat că, prin dreptul la replică transmis de instituția respectivă, unei publicații on-line locale, au fost dezvăluite date cu caracter personal care pot duce la identificarea fiicei petentei. Astfel, elementele regăsite în dreptul la replică (și anume a datei la care minora a fost instituționalizată, a unor aspecte privind paternitatea, a centrului și a perioadei la care a fost instituționalizată, a datei internării și a externării, a diagnosticului, a numărului adresei prin care a fost sesizată poliția cu privire la infracțiunea a cărei victimă a fost minora), reprezintă informații privind o persoană fizică identificabilă, conținând date de localizare și multe elemente specifice, proprii identității economice, culturale sau sociale a acesteia.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul, cu avertisment, pentru încălcarea prevederilor art. 5 alin. 1 lit. a), b), f) și alin. 2 din RGPD, precum și ale art. 6 alin. (1) din RGPD.

Totădată, Autoritatea națională de supraveghere a obligat operatorul să ia măsuri astfel încât datele cu caracter personal ale fiicei petentei să nu mai fie făcute publice, să revizuiască procedurile interne și să instruiacă personalul astfel încât, pe viitor, să se asigure conformitatea operațiunilor de prelucrare cu dispozițiile RGPD, respectiv să fie evitate astfel de situații de prelucrare a datelor cu caracter personal fără consimțământul persoanelor vizate și fără existența unei alte situații în care consimțământul nu este necesar.

F. Prelucrare date proprietari/locatari de către asociații de proprietari

O parte semnificativă a plângerilor adresate Autorității naționale de supraveghere, în anul 2021, au avut ca obiect prelucrarea nelegală a datelor cu caracter personal de către asociațiile de proprietari.

În acest context, au fost reclamate, în principal, aspecte referitoare la: afișarea la avizierul condominiului a diferite documente care conțineau date cu caracter personal ale proprietarilor, utilizarea imaginilor video preluate de sistemele de supraveghere video instalate în alt scop decât cel pentru care au fost instalate inițial camerele de supraveghere la nivelul asociației de proprietari, nerespectarea dreptului de acces la propriile imagini, instalarea nelegală a camerelor de supraveghere pe paliere.

1. FIȘĂ DE CAZ

Un petent a sesizat Autoritatea națională de supraveghere cu privire la faptul că asociația de proprietari i-a dezvăluit datele cu caracter personal (nume, prenume, domiciliu), cuprinse într-o solicitare înregistrată la asociație, prin afișarea respectivului înscris la intrările în scările blocului în care domiciliază.

Petentul a precizat că s-ar fi adresat președintelui asociației, solicitând ca datele sale personale să nu mai fie dezvăluite publicului larg, însă nu s-au luat toate măsurile pentru soluționarea cererii sale.

Totodată, din conținutul plângerii a rezultat că, alături de datele petentului, au fost dezvăluite și datele altei persoane fizice, domiciliată în același bloc.

În cadrul investigației s-a constatat că asociația de proprietari nu a facut dovada asigurării confidențialității datelor cu caracter personal ale petentului și ale unei alte persoane din imobil, dezvăluind datele cu caracter personal (nume, prenume și anumite informații legate de adresă: denumirea străzii, numărul, nr. bloc) ale acestora, prin afișarea în scara blocului a unui înscris ce conținea datele personale menționate mai sus, fără consimțământul persoanelor vizate și fără existența unei alte situații în care consimțământul nu este necesar.

La finalizarea demersurilor întreprinse, Autoritatea națională de supraveghere a sancționat operatorul cu avertisment pentru încălcarea prevederilor art. 6 din Regulamentul (UE) 2016/679.

Totodată, s-a recomandat asociației de proprietari să ia măsurile necesare astfel încât, pe viitor, să se asigure conformitatea operațiunilor de prelucrare cu dispozițiile RGPD, respectiv să fie evitate astfel de situații de prelucrare a datelor cu caracter personal fără consimțământul persoanelor vizate și fără existența unei alte situații în care consimțământul nu este necesar.

2. FIȘĂ DE CAZ

Autoritatea națională de supraveghere a întreprins demersuri pentru soluționarea plângerii depuse de un petent care a reclamat refuzul unei asociații de proprietari de a-i soluționa favorabil cererea de acces la imaginile înregistrate de camerele video instalate de aceasta și care suprind inclusiv spațiul public din exteriorul blocului.

Astfel, petentul a solicitat o copie a înregistrării video captate într-o anume perioadă de timp de sistemul de supraveghere instalat la una din scările asociației, având în vedere că în acel interval anvelopele autoturismului pe care îl folosește și care era parcat în fața acelei scări, au fost înțepate și dezumflate complet (petentul a precizat că imaginile îi sunt necesare pentru susținerea plângerii penale depuse anterior).

La cererea sa, asociația i-a răspuns că sistemul de supraveghere amplasat în interior și exterior a fost achiziționat și pus în funcțiune exclusiv de către proprietarii din scara respectivă prin intermediul unei firme specializate care a poziționat camerele de luat vederi pe direcția accesului în această scară, la solicitarea proprietarilor de la această scară, pentru siguranța și protecția lor. Petentul a revenit cu cererea de acces la imagini, invocând Regulamentul General de Protecție a Datelor și solicitând, totodată, conservarea înregistrărilor video în vederea evitării suprascrierii lor, pentru a le pune asociația la dispoziția

organelor de urmărire penală în cadrul dosarului penal. La această cerere asociația a răspuns că nu poate da curs solicitării, deoarece nu dispune de personal specializat care să utilizeze sistemul de supraveghere pentru a accesa și extrage informațiile și imaginile din perioada solicitată.

În cadrul investigației efectuate în acest caz, s-a constatat că operatorul nu a comunicat la cererile petentului informațiile solicitate în baza dreptului de acces prevăzut de art. 15 din RGPD, cu toate că, din actele prezentate, erau stabilite anumite instrucțiuni cu privire la punerea la dispoziție a imaginilor "din sistemul de supraveghere în baza unei solicitări scrise, însoțită de suportul pe care vor fi transferate înregistrările solicitate". În răspunsul trimis către Autoritatea națională de supraveghere, reprezentanții asociației au mai declarat că imaginile sunt accesate "doar în cazul solicitărilor venite din partea organelor judiciare, conform legii".

Față de cele constatate, s-a dispus aplicarea unei sancțiuni contravenționale (avertisment), pentru încălcarea art. 15 din RGPD și s-a dispus totodată ca măsură corectivă obligarea asociației de a comunica către petent un răspuns adecvat și informațiile solicitate de acesta, inclusiv imaginile cerute în măsura în care mai erau disponibile.

De asemenea, s-a pus în vedere asociației asigurarea legalității prelucrării datelor personale prin intermediul mijloacelor de supraveghere video, inclusiv sub aspectul informării persoanelor vizate, conform art. 12-14 din RGPD, al respectării drepturilor acestora, conform art. 12-22 din RGPD și al aplicării măsurilor de securitate și confidențialitate a datelor, potrivit art. 24-34 din RGPD.

CAPITOLUL IV

ACTIVITĂŢI ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE

Activitatea Autorităţii naţionale de supraveghere la nivel internațional a fost influențată și în anul 2021 de pandemia COVID-19. Prin urmare, reuniunile externe au fost organizate tot în format videoconferință, Autoritatea națională de supraveghere participând la următoarele grupuri de lucru la nivel european, conferințe, seminarii și alte reuniuni ale organismelor Uniunii Europene sau ale Consiliului Europei în domeniul protecţiei datelor cu caracter personal, precum şi prin implicarea în activitatea desfăşurată în cadrul acestora.

Acestea au inclus:

- Comitetul european pentru protecția datelor, respectiv subgrupurile de lucru: BTLE, Cooperare, Calcul amenzi, eGuvernare, Enforcement, Probleme financiare, IT users, Aspecte cheie, Social Media, Tehnologie, Transferuri Internaţionale,
- Comitetul Consultativ al Convenţiei 108 al Consiliului Europei,
- Grupul de coordonare comună în domeniul Schengen,
- Grupul de coordonare comună în domeniul Vizelor.

Comitetul european pentru protecția datelor

În anul 2021, Comitetul european pentru protecția datelor a adoptat **2** avize pe marginea proiectelor de decizie de punere în aplicare a Comisiei Europene în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Republica Coreea, respectiv Marea Britanie, **un** aviz pe marginea proiectului de decizie de punere în aplicare a Comisiei Europene în temeiul Directivei (UE) 2016/680 privind protecția adecvată a datelor cu caracter personal în Marea Britanie, **18** avize pe marginea proiectelor de decizii ale autorităților de supraveghere referitoare la regulile corporatiste obligatorii pentru operatori/persoane împuternicite de operatori, **un** aviz privind proiectul de acord administrativ cu scopul reglementării transferurilor de date cu caracter personal, **un** aviz pe marginea clauzelor contractuale standard înaintate în temeiul art. 28 alin. (8) din Regulamentul (UE) 2016/679, **5** avize 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, **7** avize pe marginea proiectului de cerințe cu privire la aprobarea criteriilor de acreditare a unui organism de certificare în conformitate cu art. 43 alin. (3) din Regulamentul (UE) 2016/679, **o** decizie obligatorie în temeiul art. 65 alin. (1) litera (a) din Regulamentul (UE) 2016/679 și **o** decizie obligatorie în temeiul art. 66 alin. (2) 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:

- Ghidul 01/2020 privind prelucrarea datelor cu caracter personal în contextul vehiculelor conectate și al aplicațiilor de mobilitate – scopul ghidului este acela de a facilita respectarea normelor privind prelucrarea legală a datelor cu caracter personal de către o gamă largă de părți interesate care își desfășoară activitatea în acest sector. De asemenea, documentul conține o serie de recomandări generale care ar trebui respectate de producătorii de vehicule și echipamente, furnizorii de servicii sau orice altă parte interesată care ar putea acționa în calitate de operator sau de persoană împuternicită de operator în legătură cu vehiculele conectate pentru a reduce riscurile pentru persoanele vizate identificate mai sus. Aceste recomandări includ aspecte privind: categoriile de date prelucrate, scopurile prelucrării, relevanța și reducerea la minimum a datelor, protecția datelor începând cu momentul conceperii și în mod implicit, informarea persoanelor vizate și drepturile acestora, securitatea datelor cu caracter personal, transmiterea datelor cu caracter personal către terți, transferul de date cu caracter personal în afara UE/SEE, utilizarea tehnologiilor Wi-Fi încorporate la bordul vehiculelor. Nu în ultimul rând, pentru a facilita înțelegerea aspectelor prezentate în ghid, acesta conține și o secțiune dedicată cazurilor practice;
- Ghidul 09/2020 privind obiecția relevantă și motivată în temeiul Regulamentului (UE) 2016/679 – scopul documentului este de a furniza orientări cu privire la conceptul de obiecție relevantă și motivată și vizează stabilirea unei interpretări comune a sintagmei „relevantă și motivată", inclusiv a criteriilor care trebuie avute în vedere atunci când se evaluează dacă o obiecție demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie;
- Ghidul 08/2020 privind direcționarea pentru adresarea de conținut personalizat către utilizatorii platformelor de comunicare socială – documentul oferă îndrumări cu privire la direcționarea conținutului către utilizatorii de platforme de comunicare socială, în special

în ceea ce privește responsabilitățile care revin inițiatorilor direcționării și furnizorilor de platforme de comunicare socială. Scopul principal al ghidului este de a clarifica rolurile și responsabilitățile care revin furnizorului de platforme de comunicare socială și inițiatorului direcționării; de asemenea, documentul identifică riscurile potențiale pentru drepturile și libertățile persoanelor fizice, principalii actori și rolurile acestora și abordează aplicarea cerințelor esențiale în materie de protecție a datelor (cum ar fi legalitatea și transparența, evaluarea impactului asupra protecției datelor etc.), precum și elementele-cheie ale acordurilor încheiate între furnizorii de platforme de comunicare socială și inițiatorii direcționării;

- Ghidul 02/2021 privind asistenții virtuali vocali – ghidul își propune să ofere îndrumări cu privire la aplicarea RGPD în contextul asistenților vocali virtuali (AVV), priviți ca servicii care înțeleg comenzile vocale și le execută sau fac legătura cu alte sisteme IT, dacă este necesar. Documentul identifică unele dintre cele mai relevante provocări legate de conformitate și oferă recomandări părților interesate relevante cu privire la modul de abordare a acestora; de asemenea, în cadrul ghidului sunt analizate patru din cele mai frecvente scopuri pentru care AVV-urile prelucrează date cu caracter personal: executarea cererilor, îmbunătățirea modelului de învățare automată folosit de AVV, identificarea biometrică și crearea de profiluri pentru conținut personalizat sau pentru publicitate;
- Ghidul 07/2020 privind conceptele de operator și persoană împuternicită de operator potrivit Regulamentului (UE) 2016/679 – acesta înlocuiește avizul anterior al Grupului de lucru Articolul 29 privind aceste concepte (WP169), în contextul în care de la intrarea în vigoare a Regulamentului (UE) 2016/679 au existat multiple întrebări cu privire la măsura în care Regulamentul (UE) 2016/679 a dus la modificări ale conceptelor de operator și persoană împuternicită de operator și, respectiv, ale rolurilor acestora. Astfel, având în vedere constatarea că aplicarea concretă a conceptelor necesită clarificări suplimentare, Comitetul european privind protecția datelor a considerat că este necesar să ofere orientări mai dezvoltate și mai specifice pentru a asigura o abordare consecventă și armonizată la nivelul UE și al SEE. Structurat în 2 părți, ghidul analizează mai întâi definițiile conceptelor de operator, operatori asociați, persoană împuternicită de operator și parte terță/destinatar, iar în partea a doua oferă orientări suplimentare privind consecințele diferitelor roluri de operator, operatori asociați și persoană împuternicită de operator;

➢ Ghidul 10/2020 privind restricțiile în temeiul Articolului 23 din Regulamentul (UE) 2016/679 – scopul ghidului este de a a oferi îndrumări cu privire la aplicarea art. 23 din Regulamentul din (UE) 2016/679. Prin conținutul său, acesta oferă o analiză amănunțită a criteriilor de aplicare a restricțiilor, evaluările care trebuie să fie respectate, modul în care persoanele vizate își pot exercita drepturile odată ce restricția este ridicată și consecințele încălcării art. 23 din Regulamentul din (UE) 2016/679;

➢ Avizul nr. 39/2021 privind posibilitatea ca Articolul 58 alineatul (2) RGPD să servească drept temei pentru ca o autoritate de supraveghere să dispună ex officio ștergerea datelor personale, în situația în care o astfel de cerere nu a fost depusă de persoana vizată – adoptat la cererea Autorității de Supraveghere din Ungaria, documentul prezintă decizia Comitetului european pentru protecția datelor privind această chestiune, decizie ce a fost în sensul că art. 58 alin. (2) litera g) din Regulamentul (UE) 2016/679 reprezintă un temei legal valabil pentru ca o autoritate de supraveghere să dispună ex officio ștergerea datelor personale, în situația în care o astfel de cerere nu a fost depusă de persoana vizată;

➢ Avizul 32/2021 referitor la Proiectul de decizie de punere în aplicare a Comisiei în temeiul Regulamentului (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Republica Coreea – documentul reprezintă evaluarea efectuată de Comitetul european privind protecția datelor în legătură cu nivelul de protecție adecvat asigurat în Republica Coreea, evaluare ce a fost realizată în baza examinării proiectului de decizie ca atare, precum și în baza analizării documentației puse la dispoziție de Comisia Europeană, pe baza Criteriilor de referință privind caracterul adecvat al nivelului de protecție în temeiul Regulamentului (UE) 2016/679 adoptate în februarie 2018 și a Recomandărilor 02/2020 ale Comitetului european privind protecția datelor în legătură cu garanțiile esențiale europene pentru măsurile de supraveghere. Axat atât pe evaluarea aspectelor generale legate de Regulamentul (UE) 2016/679 din proiectul de decizie, cât și pe accesul autorităților publice la datele cu caracter personal transferate din SEE în scopuri de aplicare a legii și de securitate națională, inclusiv căile de atac pe care le au la dispoziție persoanele fizice din SEE, avizul evaluează inclusiv dacă garanțiile oferite pe baza cadrului juridic coreean sunt puse în aplicare și funcționează;

➢ Avizul 15/2021 referitor la Proiectul de decizie de punere în aplicare a Comisiei în temeiul Directivei (UE) 2016/680 privind protecția adecvată a datelor cu caracter personal în Regatul Unit – utilizând ca referințe principale Criteriile de referință privind caracterul adecvat

al nivelului de protecție adoptate în februarie 2021, precum și jurisprudența relevantă reflectată în Recomandarea CEPD 02/2020, Comitetul european pentru protecția datelor a subliniat că, deși Regatul Unit are capacitatea de a recunoaște teritorii ca oferind un nivel adecvat de protecție a datelor, acest aspect ar putea duce la posibile riscuri în ceea ce privește protecția oferită datelor cu caracter personal transferate din UE mai ales dacă, în viitor, cadrul de protecție a datelor din Regatul Unit se abate de la acquis-ul UE;

- Avizul 14/2021 referitor la Proiectul de decizie de punere în aplicare a Comisiei în temeiul Regulamentul (UE) 2016/679 privind protecția adecvată a datelor cu caracter personal în Regatul Unit – analiza Comitetului european pentru protecția datelor s-a concentrat pe evaluarea atât a aspectelor generale din Regulamentul (UE) 2016/679 ale proiectului de decizie, cât și pe accesul autorităților publice la datele cu caracter personal transferate din SEE în scopul aplicării legii și securității naționale, inclusiv căile de atac disponibile persoanelor fizice în SEE. De asemenea, Comitetul european pentru protecția datelor a evaluat dacă garanțiile prevăzute în cadrul legal al Regatului Unit sunt în vigoare și eficiente;

- Recomandările nr. 01/2020 privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal – documentul a fost adoptat pentru a sprijini exportatorii de date cu caracter personal (fie ei operatori sau persoane împuternicite de operator) cu sarcina complexă de a evalua țări terțe și de a identifica măsuri suplimentare adecvate, acolo unde este necesar. Recomandările oferă acestora îndrumări cu privire la pașii de urmat, surse potențiale de informații și câteva exemple de măsuri suplimentare care ar putea fi puse în aplicare;

- Recomandările nr. 02/2021 privind temeiul juridic pentru stocarea datelor referitoare la cărțile de credit în scopul unic de a facilita alte tranzacții on-line – recomandările se referă la stocarea datelor referitoare la cărțile de credit de către furnizorii on-line de bunuri și servicii, în scopul unic și specific de a facilita achizițiile ulterioare ale persoanelor vizate și privesc, în principiu, situația în care o persoană vizată cumpără un produs sau plătește un serviciu prin intermediul unui site sau al unei aplicații și furnizează datele referitoare la cartea sa de credit, pentru a încheia respectiva tranzacție unică;

- Recomandările 01/2021 cu privire la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de aplicare legii – axat exclusiv pe deciziile privind caracterul adecvat al nivelului de protecție,

documentul urmărește să ofere orientări cu privire la nivelul de protecție a datelor în țările terțe și în organizațiile internaționale în temeiul Directivei privind protecția datelor în materie de aplicare legii. În acest context, sunt stabilite principiile fundamentale de protecție a datelor care trebuie să fie prezente în cadrul juridic al unei țări terțe sau al unei organizații internaționale pentru a asigura echivalența esențială cu cadrul UE în domeniul de aplicare al Directivei;

- Lista de prezentare generală a regulilor corporatiste obligatorii (BCR) adoptate înainte de RGPD – documentul conține informații privind regulile corporatiste obligatorii (BCR) care au fost transmise Autorităților naționale de supraveghere în vederea aprobării anterior datei de 25 mai 2018 și pentru care procedura de cooperare informală a fost încheiată cu succes, precum și informații privind autoritățile de supraveghere care au coordonat respectivele proceduri de consultare informală;
- Declarația 04/2021 privind acordurile internaționale, inclusiv transferuri – declarația a fost adoptată în contextul primirii de către Comitetul european privind protecția datelor și autoritățile naționale de supraveghere de diverse întrebări privind schimburile de date cu caracter personal dintre autoritățile publice în baza acordurilor internaționale existente în diferite domenii;
- Prezentare generală a resurselor puse la dispoziția Autorităților pentru Protecția Datelor de către Statele Membre și a acțiunilor de punere în aplicare a legii de către Autoritățile pentru Protecția Datelor – redactat la solicitarea Comisiei pentru libertăți civile, justiție și afaceri interne (Comisia LIBE) a Parlamentului European, documentul prezintă o serie de date privind resursele de care dispun autoritățile de supraveghere din statele membre în desfășurarea activității lor;

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

- Orientările 5/2021 privind interacțiunea dintre aplicarea Articolului 3 și dispozițiile privind transferurile internaționale conform capitolului V din RGPD;
- Orientările 04/2021 privind codurile de conduită ca instrumente pentru transferuri;
- Orientările 3/2021 privind aplicarea Articolului 65 alineatul (1) litera a) din RGPD;
- Orientările privind evaluarea criteriilor de certificare (anexă la Orientările 1/2018 privind privind certificarea și identificarea criteriilor de certificare în conformitate cu Articolele 42 și 43 din Regulament;

➢ Orientările 1/2021 privind exemplele de notificare a încălcărilor securității datelor cu caracter personal.

De asemenea, Comitetul european pentru protecția datelor a adoptat o serie de **avize comune**, împreună cu Autoritatea Europeană pentru Protecția Datelor, după cum urmează:

➢ Avizul comun nr. 1/2021 al CEPD-AEPD referitor la Decizia de punere în aplicare a Comisiei Europene privind clauzele contractuale standard dintre operatori și persoanele împuternicite de operatori pentru aspectele menționate la Articolul 28 alineatul (7) din Regulamentul (UE) 2016/679 și la Articolul 29 alienatul (7) din Regulamentul (UE) 2018/1725 – avizul CEPD și AEPD a avut drept scop asigurarea coerenței și a aplicării corecte a art. 28 din Regulamentul (UE) 2016/679 în ceea ce privește proiectul de clauze contractuale standard prezentat, care ar putea servi drept clauze contractuale standard în conformitate cu art. 28 alin. (7) din Regulamentul (UE) 2016/679 și cu art. 29 alin. (7) din Regulamentul (UE) 2018/1725;

➢ Avizul comun nr. 2/2021 al CEPD-AEPD referitor la Decizia de punere în aplicare a Comisiei Europene privind clauzele contractuale standard pentru transferul de date cu caracter personal către țări terțe pentru aspectele menționate la art. 46 alin (2) litera c) din Regulamentul (UE) 2016/679 – elaborat la cerere Comisiei Europene, avizul comun al CEPD și AEPD cuprinde (i) o parte principală care detaliază observațiile generale pe care CEPD și AEPD doresc să le formuleze și (ii) o anexă în care se fac observații suplimentare cu caracter mai tehnic în legătură directă cu proiectul de clauze contractuale standard, în special pentru a oferi câteva exemple de posibilele modificări. Deși au constatat că proiectul de clauze contractuale standard reflectă mai multe măsuri identificate în Recomandările CEPD privind măsurile suplimentare, pentru alte prevederi CEPD și AEPD au solicitat o mai mare coerență și o serie de clarificări din partea Comisiei cu privire la conținutul acestora;

➢ Avizul comun nr. 3/2021 al CEPD-AEPD privind Propunerea de regulament European și al Consiliului privind guvernanța datelor la nivel european (Legea privind guvernanța datelor) – avizul a fost elabroat de CEPD și AEPD plecând de la premisa că scopul său nu este de a enumera exhaustiv aspectele care trebuie abordate de legiuitori, și nici de a face propuneri alternative sau sugestii de formulare pentru fiecare dintre acestea, ci de a urmări abordarea principalelor aspecte critice ale propunerii;

➢ Avizul comun nr. 4/2021 al CEPD-AEPD referitor la propunerea de Regulament al Parlamentului European și al Consiliului privind un cadru pentru eliberarea, verificarea și

acceptarea certificatelor interoperabile de vaccinare, de testare și de vindecare în vederea facilității liberei circulații în timpul pandemiei de COVID-19 (certificatul verde digital) – prin acest aviz, CEPD și AEPD au formulat o serie de observații specifice privind protecția datelor în legătură cu certificatul verde digital, subliniind cu titlu general că această propunere nu permite – și nu trebuie să conducă – la crearea niciunei baze centrale de date cu caracter personal la nivelul UE sub pretextul instituirii cadrului privind certificatele verzi digitale;

- Avizul comun nr. 5/2021 al CEPD-AEPD privind propunerea de Regulament al Parlamentul European și al Consiliului de stabilire a unor norme armonizate privind inteligenta artificială (Legea privind inteligenta artificială) – prin avizul comun, CEPD și AEPD analizează prioncipiile-cheie ale propunerii de regulament și interacțiunea cu cadrul de protecția a datelor. De asemenea, deși salută propunerea Comisiei și consideră că un astfel de regulament este necesar pentru a garanta drepturile fundamentale ale cetățenilor și rezidenților UE, CEPD și AEPD apreciază că propunerea trebuie revizuită în mai multe privințe, pentru a asigura aplicabilitatea și eficiența acesteia, concluzionând că mai rămân multe de făcut până când propunerea poate da naștere unui cadru juridic funcțional, care să completeze în mod eficient Regulamentul (UE) 2016/679 în ceea ce privește protejarea drepturilor fundamentale ale omului, promovând în același timp inovarea.

Comitetul Consultativ al Convenției 108 al Consiliului Europei

Obiectivul Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108) este protejarea dreptului la viață privată, aceasta prevăzând încorporarea de către părți, în legislațiile naționale, a măsurilor necesare pentru a garanta că tuturor persoanelor le sunt respectate drepturile în ceea ce privește protecția datelor cu caracter personal. Convenția 108 a fost semnată în anul 1981, iar evoluțiile în domeniul tehnologic și-au pus amprenta și asupra acestui instrument juridic, ceea ce a condus la nevoia de a actualiza dispozițiile sale. În atare situație, în luna mai 2018, Comitetul de Miniști al Consiliului Europei a adoptat Protocolul de amendare a Convenției 108, acesta fiind deschis spre semnare începând cu data de 10 octombrie 2018.

În vederea consolidării dreptului la protecția datelor cu caracter personal, în cursul anului 2021 Ministerul Afacerilor Externe a inițiat, împreună cu Autoritatea națională de supraveghere, Proiectul de lege pentru ratificarea Protocololul adoptat la Strasbourg, la 10 octombrie 2018, de amendare a Convenției pentru protejarea persoanelor față de prelucrarea

automatizată a datelor cu caracter personal, adoptată la Strasbourg, la 28 ianuarie 1981, protocol ce a fost semnat de România la 26 iunie 2020.

Prin ratificarea Protocolului de amendare a Convenției 108 și intrarea acestuia în vigoare, România a devenit parte la Convenția 108 modernizată.

Noutățile pe care le aduce Convenția 108 modernizată prin intermediul Protocolului de amendare vizează introducerea unor garanții cum ar fi principiul proporționalității – în special minimizarea datelor, principiul responsabilității – prin responsabilizarea operatorilor și persoanelor împuternicite de operatori, asigurarea protecției datelor cu caracter personal începând cu momentul conceperii – privacy by design, garanții suplimentare pentru persoanele vizate – precum dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrare automată, dreptul la opoziție, dar și posibilitatea organizațiilor internaționale de a adera la Convenția 108 modernizată – creându-se astfel premisele unei viitoare aderări a UE.

Convenția 108 modernizată include garanții care sunt în mare parte similare cu cele reglementate în dreptul UE, în principal prin intermediul Regulamentului (UE) 2016/679, scopul său fiind acela de a contribui la promovarea generală a standardelor UE în domeniul protecției datelor la nivel internațional.

Proiectul de lege a fost adoptat de Parlament în cursul lunii noiembrie 2021 și, ulterior, promulgat de Președintele României, devenind astfel Legea nr. 290/2021 pentru ratificarea Protocolului adoptat la Strasbourg, la 10 octombrie 2018, semnat de România la 26 iunie 2020, de amendare a Convenţiei pentru protejarea persoanelor faţă de prelucrarea automatizată a datelor cu caracter personal, adoptată la Strasbourg, la 28 ianuarie 1981.

Grupul de coordonare comună în domeniul Schengen

La ultima reuniune a Grupului de coordonare comună a fost evidențiată creșterea alertelor referitoare la supravegherea discretă în temeiul art. 36 Decizia 2007/533/JAI privind înfiinţarea, funcţionarea şi utilizarea Sistemului de informaţii Schengen de a doua generaţie (SIS II).

Luând în considerare ultimele statistici prezentate în raportul eu-LISA, a reieșit faptul că a existat o creștere destul de mare (aproximativ 10%), în anul 2021 înregistrându-se un număr de 129983 de alerte în temeiul art. 36, ceea ce reprezintă 15% din numărul total de alerte privind persoanele din SIS.

Astfel, Grupul de coordonare comună a decis desfășurarea unei activități coordonate prin completarea unui chestionar, scopul acestui exercițiu fiind conștientizarea referitoare la informații și statistici specifice cu privire la utilizarea alertelor prevăzute la art. 36 de către autoritățile competente.

Grupul de coordonare comună în domeniul Vizelor

Sistemul privind vizele prevede termene stricte pentru păstrarea datelor cu caracter personale, termenele fiind diferite pentru fiecare categorie de date, dar principiul fiind același: ștergerea este efectuată automat de Unitatea Centrală la expirarea perioadei legale de păstrare.

Ștergerea anticipată contribuie, de asemenea, la o gestionare corectă a bazelor de date la scară largă. Verificările anterioare au arătat că o serie de date ar fi trebuit șterse dintr-o varietate de motive (ștergerea alertei, rectificarea obținută de persoana vizată etc.). Atunci când ștergerea nu este executată în mod activ, poate crea probleme serioase pentru persoana vizată, dar și pentru funcționarea sistemului, din cauza inexactității datelor.

Chestiunea în contextul vizelor este că ștergerea anticipată nu este întotdeauna asigurată într-un mod adecvat și consecvent în statele membre.

Astfel, la nivelul grupului s-a decis realizarea unui exercițiu prin care să se examineze dacă și în ce mod ștergerea anticipată este realizată de autoritățile naționale competente. Acest exercițiu explorator are drept obiectiv identificarea de bune practici și încurajarea utilizării lor, precum și emiterea de recomandări în situația în care există deficiențe în sistemul actual.

Reguli Corporatiste Obligatorii

Un aspect important în ceea ce privește transferurile internaționale de date cu caracter personal este reprezentat de evaluarea și aprobarea cererilor de reguli corporatiste obligatorii transmise de companii multinaționale. De asemenea, Autoritatea națională de supraveghere are un rol consultativ în privința transferurilor de date, indiferent de temeiul legal al acestora.

Regulile corporative obligatorii (BCRs) au fost introduse ca răspuns la nevoia organizațiilor de a avea o abordare globală în ceea ce privește protecția datelor cu caracter personal, în situația în care multe organizații dețineau mai multe filiale/sucursale situate pe tot globul, transferând date cu caracter personal la scară largă. Includerea BCRs în

Regulamentul (UE) 2016/679 consolidează în continuare utilizarea lor ca garanție adecvată pentru a legitima transferurile de date cu caracter personal în țări terțe.

În anul 2021, Autoritatea națională de supraveghere a primit și a analizat cereri de aprobare a BCRs transmise de 40 de companii multinaționale. De asemenea, Autoritatea națională de supraveghere a acționat în calitate de autoritate principală pentru 2 seturi de reguli corporatiste obligatorii și a asistat alte autorități de supraveghere, acționând în calitate de co-revizor la cererile de aprobare a BCRs transmise de 5 companii în această perioadă și ca membru în echipa de redactare a unei 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:

- includerea de mențiuni referitoare la obligația de a răspunde la cererile de exercitare a drepturilor persoanei vizate;
- includerea de mențiuni referitoare la accesul autorităților publice la datele cu caracter personal;
- specificarea mențiunilor prezentate la art. 28 din Regulamentul (UE) 2016/679, cu precădere alin. (2) (autorizație scrisă, specifică sau generală, din partea operatorului atunci când persoana împuternicită de operator recrutează o altă persoană împuternicită);
- includerea de mențiuni referitoare la notificarea noilor sub-împuterniciți;
- includerea de mențiuni referitoare la oferirea de suport operatorului în vederea asigurării respectării obligațiilor prevăzute la art. 32-36 din Regulamentul (UE) 2016/679;
- informarea imediată a operatorului în situația în care o instrucțiune încalcă Regulamentul (UE) 2016/679;
- respectarea obligației prevăzute de art. 30 din Regulamentul (UE) 2016/679;
- introducerea unei noi secțiuni privind actualizarea regulilor corporatiste obligatorii;
- păstrarea unei evidențe a cererilor de exercitare a drepturilor de la persoanele vizate;
- păstrarea unei evidențe a plângerilor primite de la persoanele vizate;
- întocmirea de către responsabilul cu protecția datelor a unui raport referitor la plângerile primite, obiectul plângerilor, precum și rezultatul soluționării acestora.

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 2021, Comitetul european pentru protecția datelor a emis 18 opinii 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 intermeniul sistemului IMI

În contextul cooperării cu alte autorități de supraveghere din UE în vederea asigurării asistenței reciproce, au fost gestionate aproximativ **35 solicitări** cu privire la aplicarea și respectarea Regulamentul (UE) 2016/679. Solicitările venite din partea autorităților de supraveghere din Finlanda, Franța, Germania, Letonia, Malta, Olanda, Polonia, Spania, Ungaria au vizat, în principal, aspecte referitoare la stocarea datelor biometrice, invocarea secretului profesional, argumentele care stau la baza emiterii unei decizii de ștergere a datelor cu caracter personal prelucrate ilegal, supravegherea video a personalului de pază, implementarea art. 78 alin. (2) din Regulamentul (UE) 2016/679, implementarea art. 85 din Regulamentul (UE) 2016/679, prelucrarea datelor cu caracter personal din certificatul COVID-19 în alte scopuri, implementarea prevederilor Directivei (UE) 2018/1972, competențele Autorității naționale de supraveghere în domeniul securității naționale și accesul la informațiile clasificate, prelucrarea datelor cu caracter personal prin intermediul dispozitivelor medicale interconectate, temeiul legal utilizat pentru scraping software.

Contribuții pe marginea documentelor din perspectiva protecției datelor cu caracter personal

În cursul anului 2021, Autoritatea națională de supraveghere a formulat observații și propuneri pe marginea documentelor transmise de alte autorități/instituții:

- raportul anual 2020 și planul de lucru 2022 al Agenției pentru Drepturi Fundamentale a Uniunii Europene – Autoritatea națională de supraveghere a transmis comentarii pe marginea celor două documente transmise spre analiză, cu incidență asupra capitolului care vizează domeniul protecției datelor cu caracter personal;
- proiectul de Regulament privind piețe contestabile și echitabile în sectorul digital – Autoritatea națională de supraveghere a transmis o serie de observații pe marginea documentului înaintat referitoare la definirea conceptului de „consimțământ", drepturile persoanelor vizate, în special al dreptului la portabilitatea datelor prevăzut de art. 20 din Regulamentul (UE) 2016/679;
- propunerea de Regulament privind guvernanța datelor la nivel european – Autoritatea națională de supraveghere a formulat o serie de observații referitoare la aplicabilitatea definițiilor prevăzute la art. 4 din Regulamentul (UE) 2016/679 și în conextul guvernanței datelor, cu mențiunea că noile definiții introduse, în măsura în care se referă la prelucrarea datelor cu caracter personal, nu ar trebuie să conțină reguli care sunt incompatibile cu Regulamentul (UE) 2016/679, existența unei distincții clare între date cu caracter personal și date nepersonale, pentru a evita confuzia cu privire la modul în care propunerea de regulamentul s-ar aplica cu respectarea prevederilor Regulamentului (UE) 2016/679, menționarea în mod expres a temeiului legal pentru prelucrarea datelor cu caracter personal, așa cum este prevăzut de Regulamentul (UE) 2016/679.

În același timp, Autoritatea națională de supraveghere a evidențiat faptul că, în cazul prelucrărilor de date cu caracter personal, „permisiunea" menționată în propunerea de regulament nu poate înlocui necesitatea existenței unuia dintre temeiurile legale prevăzute la art. 6 alin. (1) și art. 9 alin. (2) din Regulamentul (UE) 2016/679 în măsura în care se prelucrează categorii speciale de date, astfel încât prelucrarea să fie legală. Deci, prelucrarea datelor cu caracter personal este legală numai dacă și în măsura în care se aplică cel puțin unul dintre temeiurile prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679.

De asemenea, în ceea ce privește condițiile de reutilizare prevăzute la art. 5 din propunere, în conformitate cu principiul legalității prelucrării stabilit la art. 5 alin. (1) lit. a) din Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere a recomandat clarificarea faptului că un temei legal corespunzător potrivit Regulamentului (UE) 2016/679 trebuie prevăzut în legislația Uniunii sau a statelor membre și trebuie identificat cu atenție de către organismele din sectorul public cu privire la orice reutilizare ulterioară a datelor cu caracter personal. În același timp, nu a fost identificată obligația organismelor din sectorul privat de a realiza informarea persoanelor vizate (principiul transparenței) prevăzută de Regulamentul (UE) 2016/679, recomandându-se astfel includerea unei dispoziții explicite referitoare la obligația acestor entități din sectorul public de a realiza informarea persoanelor vizate în temeiul Regulamentului (UE) 2016/679, astfel încât să se asigure exercitarea drepturilor conferite persoanelor vizate în temeiul legislației în domeniul protecției datelor.

Totodată, a fost evidențiată necesitatea respectării și a celorlalte principii prevăzute de art. 5 din Regulamentul (UE) 2016/679, în special principiul reducerii la minimum a datelor și principiul integrității și confidențialității. De asemenea, Autoritatea națională de supraveghere a atras atenția asupra necesității implementării de măsuri tehnice și organizatorice adecvate, în conformitate cu art. 24 din Regulamentul (UE) 2016/679, precum și a respectării principiului asigurării protecției datelor începând cu momentul conceperii și în mod implicit (privacy by design and by default), statuat de art. 25 din Regulamentul (UE) 2016/679;

➢ propunerea de Regulament al Parlamentului European și a Consiliului de modificare a Regulamentului (UE) 2016/794 (Regulamentul Europol) – Autoritatea națională de supraveghere a transmis o serie de observații cu privire la necesitatea definirii termenilor utilizați în domeniul protecției datelor, notificarea în cazul încălcărilor securității datelor cu caracter personal, extinderea perioadei de stocare a datelor cu caracter personal, respectarea principiilor legate de prelucrarea datelor cu caracter personal, în special principiul limitării legate de scop. De asemenea, au fost solicitate informații suplimentare/clarificări referitoare la datele personale/categoriile de date personale avute în vedere a fi prelucrate în scop de cercetare și inovare, respectiv ce activități de cercetare și inovație au fost avute în vedere, informații suplimentare cu privire la consecințele eliminării articolului care reglementa înființarea Consiliului de Cooperare Europol, respectiv care va fi forma de cooperare dintre EDPS și autoritățile de supraveghere naționale, clarificări cu privire introducerea posibilității

Europol de a solicita date personale de la entități private, clarificări cu privire la extinderea perioadei de păstrare fișierelor de înregistrare (log-uri);

- propunerea de directivă privind transparența salarială – Autoritatea națională de supraveghere a solicitat clarificări în legatură cu accesul reprezentanților salariaților/sindicatului la categoria de date cu caracter personal – salariul. În această privință, Autoritatea națională de supraveghere a subliniat faptul că, în jurisprudenta sa, CCR, prin Decizia nr. 615/2006, a reținut că salariul concret al unei persoane, stabilit în cadrul limitelor minime și maxime prevăzute în actele normative, ținând seama de importanța muncii depuse, de contribuția adusă la realizarea sarcinilor și de situația sa personală intră în sfera interesului privat al persoanei;

- propunerea de regulament privind certificate verzi digitale – Autoritatea națională de supraveghere a transmis o serie de observații pe marginea propunerii de regulament care vizau, în principal, aplicabilitatea definițiilor prevăzute de Regulamentul (UE) 2016/679, specificarea în mod clar a categoriilor de date cu caracter personal referitoare la identificarea persoanei, cu respectarea, în același timp, a principiului privind reducerea la minimum a datelor, necesitatea menționării tuturor categoriilor de metadate, pentru a asigurea claritatea textului, enumerarea fiind limitativă și nu exemplificativă, prin raportare la necesitarea respectării principiului proporționalității, necesitatea respectării prevederilor de la art. 24, art. 25 și art. 32 din Regulamentul (UE) 2016/679, necesitatea stabilirii unei perioade de stocare a datelor personale prelucrate în scopul emiterii certificatelor, prin raportare la principiul limitării legate de stocare, precum și în vederea asigurării unei abordări unitare la nivelul statelor membre, necesitatea includerii de dispoziții referitoare la drepturile persoanelor vizate, la autoritatea responsabilă pentru monitorizarea legalității prelucrării datelor cu caracter personal.

De asemenea, au fost solicitate informații suplimentare cu privire la „autoritățile responsabile pentru emiterea certificatelor" și cu privire la specificitațile tehnice aplicabile până la data adoptării de către Comisia Europeană a actelor de implementare, astfel încât să se asigure uniformitatea la nivelul statelor membre;

- chestionarul privind implementarea art. 78 și 85 din Regulamentul (UE) 2016/679 și a art. 53 din Directiva (UE) 2016/680 transmis de Comisia Europeană;

- elemente de mesaj cu privire la transferurile de date cu caracter personal către state terțe și revizuirea clauzelor contractuale standard – în absența unei decizii privind

caracterul adecvat al nivelului de protecție, transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate. În atare situație, în absența unei decizii privind caracterul adecvat în temeiul art. 45 alin. (3) din Regulamentul (UE) 2016/679, transferul de date cu caracter personal către țări terțe sau organizații internaționale poate fi efectuat în conformitate cu unul din următoarele instrumente prevăzute de art. 46 din Regulamentul (UE) 2016/679: clauze standard de protecție a datelor, reguli corporatiste obligatorii, coduri de conduită și mecanisme de certificare.

De asemenea, Autoritatea națională de supraveghere a menționat faptul că datele cu caracter personal pot fi transferate în baza derogărilor prevăzute la art. 49 din Regulamentul (UE) 2016/679, cu condiția să se aplice condițiile prevăzute în respectiva dispoziție. În acest context, a fost subliniat faptul că transferul de date cu caracter personal se realizează cu respectarea obligațiilor ce revin operatorului de date/exportatorului de date (respectarea si demonstrarea respectării condițiilor de legalitate, a principiilor de prelucrare, a măsurilor de confidențialitate și securitate a datelor cu caracter personal pentru a asigura protecția acestora, respectarea drepturilor persoanelor vizate).

CAPITOLUL V

MANAGEMENTUL ECONOMIC AL AUTORITĂȚII

În vederea desfăşurării activităţii, Autorității naționale de supraveghere i s-a alocat prin Legea nr. 15/2021 a bugetului de stat pe anul 2021 un buget inițial în sumă de 5.039.000 lei, modificat în conformitate cu prevederile Ordonanţei de urgență a Guvernului nr. 97/2021 cu privire la rectificarea bugetului de stat pe anul 2021 și Ordonanţei de urgență a Guvernului nr. 122/2021 cu privire la rectificarea bugetului de stat pe anul 2021 şi la instituirea cadrului legal pentru acordarea unui împrumut subordonat de către statul român, prin Ministerul Finanţelor, în calitate de acţionar, către CEC Bank - S.A.

Evoluția sumelor alocate pentru bugetul Autorității naționale de supraveghere în ultimii 5 ani poate fi observată în tabelul de mai jos:

Comparație buget anual 2017-2021

Anul	2017	2018	2019	2020	2021
Buget final (mii lei)	4.287	4.735	5.147	4.903	4.601
% față de anul anterior	88	110,45	108,70	95,26	93,84

Bugetul anului 2021 a fost mai mic cu aproximativ 6% față de bugetul anului anterior. Dat fiind faptul că modul de concepere a bugetelor pune un accent semnificativ pe sumele cheltuite anterior, din cauza numarului mic de personal și a faptului că sumele necesare depășesc semnificativ alocările anterioare la capitolul investiții, bugetele aprobate Autorității naționale de supraveghere au ramas la un nivel care asigură doar funcționarea nu și dezvoltarea acestei instituții.

Considerăm necesar să amintim faptul că și restricțiile aferente perioadei de pandemie Covid-19 au afectat bugetul și cheltuielile anului 2021, atât prin limitarea deplasărilor în țară și străinătate, cât și prin micșorarea cheltuielilor administrative (pe fondul măsurilor dispuse pentru limitarea efectelor pandemiei și răspândirii virusului).

Având în vedere aceste aspecte și în urma anulărilor de credite realizate în luna decembrie 2021, conform reglementărilor Legii nr. 500/2002 privind finanţele publice, cu modificările și completările ulterioare, rezultă următoarea sinteză:

Denumire indicator	Cod	Buget iniţial 2021 - mii lei -	Buget final (actualizat la 31.12.2021) - mii lei -	Execuție bugetară la 31.12.2021 - mii lei -	Execuţie bugetară la 31.12.2021 (%)
Total cheltuieli	**51.01**	**5.039**	**4.601**	**4.537**	**98,61**
Titlul I Cheltuieli de personal	**10**	**4.059**	**3.776**	**3.757**	**99,50**
Titlul II Bunuri şi servicii	**20**	**880**	**740**	**707**	**95,55**
Cheltuieli de capital Titlul XIII Active nefinanciare	**71**	**100**	**85**	**76**	**89,42**

Întrucât pe parcursul exercițiului bugetar au avut loc rectificări bugetare, s-a urmărit permanent actualizarea priorităților pentru realizarea celor mai importante proiecte cu fondurile disponibile.

După cum menționam și anterior, un impact major asupra activităților instituției s-a înregistrat și în anul 2021 din cauza pandemiei COVID-19, în această perioadă fiind anulate deplasările personalului și existând o preocupare permanentă pentru limitarea expunerii la îmbolnăvire a salariaților.

În acest context, s-au luat și numeroase măsuri organizatorice, conform recomandărilor Ministerului Muncii în scopul prevenirii răspândirii infectării cu Coronavirus, precum modificarea temporară a locului de muncă la domiciliul salariatului pe durata stării de urgență ori flexibilizarea programului de lucru.

De asemenea, unele achiziții nu au putut fi realizate datorită modificărilor din piața de bunuri și servicii generate de pandemie (probleme cu aprovizionarea cu materii prime, probleme de logistică și transport).

În acest context, creditele definitive aprobate au asigurat continuitatea activității Autorității naționale de supraveghere, în contextul măsurilor luate în scopul prevenirii răspândirii infectării cu Coronavirus și ale măsurilor interne dispuse de conducerea instituției privind utilizarea eficientă a fondurilor publice.

În ceea ce privește modul de repartizare a fondurilor alocate, este de precizat faptul că suma aferentă cheltuielilor de personal ale Autorității naționale de supraveghere a constituit un procent de 82,07% din totalul creditelor repartizate de la bugetul de stat, sumă din care s-au utilizat efectiv credite în valoare de 3.757.978 lei.

Autoritatea națională de supraveghere a înregistrat, în continuare, un deficit major de personal, numărul posturilor ocupate fiind de 1/3 din totalul prevăzut de Legea nr. 102/2005, republicată, (doar 29 posturi ocupate la debutul anului și 33 posturi ocupate la finalul anului 2021 – inclusiv demnitarii – din totalul de 87 posturi prevăzute de lege).

Având în vedere deficitul extrem de mare de personal din cadrul Autorității naționale de supraveghere, în anul 2021 au fost organizate 2 concursuri pentru ocuparea unor posturi vacante, însă, cu toate eforturile depuse de Autoritatea națională de supraveghere, pentru unele posturi vacante nu a fost depus niciun dosar de concurs, astfel încât, la finalul anului 2021, numărul de personal al instituției a crescut cu doar 4 salariați.

În ceea ce privește majoritatea cheltuielilor de personal, este de menționat că acestea au fost aferente plăților efectuate pentru munca salariată a angajaților din compartimentele de specialitate.

Cheltuielile aferente Titlului II Bunuri și servicii în anul 2021 au avut o pondere de 16,09% în bugetul instituției, iar din acestea, cheltuielile mai importante au fost:

I. aproximativ 46 % din totalul sumelor achitate din conturile de trezorerie ale Autorității naționale de supraveghere la Titlul II Bunuri și servicii au fost reprezentate de costurile de închiriere și cheltuielile cu utilitățile și serviciile prestate de RA-APPS prin intermediul SAIFI,
II. diferența până la 100% este reprezentată de cheltuieli cu bunuri și servicii pentru întreținere și funcționare (servicii de actualizare informatică, servicii de suport

tehnic, instalare și configurare software, actualizarea sistemului electronic de gestiune a documentelor Folium, curățenie, cheltuieli cu serviciile poștale și de telefonie, cheltuieli generate de pandemie, abonament program legislativ, furnituri de birou și alte materiale necesare desfășurării activității etc.).

În anul 2021, cheltuielile cu bunuri și servicii au scăzut cu 7 % față de anul 2020, în contextul pandemiei de coronavirus (execuția bugetară la Titlul II Bunuri și servicii fiind de 707 mii lei în anul 2021, față de 757 mii lei în anul 2020).

Pe parcursul exercițiului bugetar 2021, datorită unor circumstanțe neprevăzute (precum eliminarea restricțiilor privind realizarea concursurilor pentru ocuparea posturilor vacante care a generat modificarea numărului de personal ori necesitatea remedierii urgente a unor vulnerabilități constatate la sistemul IT) necesarul de fonduri s-a modificat, iar lista de investiții a suferit schimbări față de estimările inițiale, ceea ce a determinat o execuție bugetară semnificativ diferită față de previziunile realizate cu prilejul întocmirii proiectului de buget pe anul 2021.

De asemenea, trebuie precizat că, în măsura în care acest lucru a fost posibil, s-au avut permanent în vedere factori precum: oportunitatea cheltuielilor, criteriul prețului celui mai scăzut aplicat în procedurile de achiziții publice, alăturat unor cerințe tehnice atent stabilite – ceea ce a condus la utilizarea eficientă a fondurilor bugetare alocate atât la Titlul II Bunuri și servicii, cât și la Titlul XIII Active nefinanciare.

În ceea ce privește Titlul XIII Active nefinanciare, în anul 2021 Autoritatea națională de supraveghere a continuat, în măsura posibilităților oferite de alocările bugetare și de urgențele generate de unele vulnerabilități ale sistemului IT, proiectul de reînnoire a infrastructurii, în aceste scopuri fiind utilizate fondurile prevăzute în bugetul final al Titlului Cheltuieli de capital. Acest proiect continuă să fie deosebit de important, funcționarea sistemului IT fiind esențială în contextul trecerii într-o proporție tot mai mare a activității în mediul on-line datorită pandemiei și a tendințelor de la nivel intern și internațional.

Politicile contabile utilizate la întocmirea situațiilor financiare anuale sunt în conformitate cu reglementările legale în vigoare, iar situațiile financiare anuale oferă o imagine fidelă a realității poziției financiare a Autorității naționale de supraveghere, precum și informații privind încadrarea în creditele bugetare alocate pe grupe, titluri, articole și alineate de cheltuieli, așa cum sunt prevăzute acestea în bugetul instituției noastre.

Cheltuielile bugetare s-au efectuat cu respectarea principiilor privind legalitatea, oportunitatea, continuitatea şi eficienţa. Toate documentele care intră sub incidenţa controlului financiar preventiv propriu au fost verificate şi vizate pentru conformitate/încadrare în limitele bugetare.

Ca o concluzie asupra gestionării fondurilor bugetare alocate, putem preciza că acestea au fost utilizate cu maximum de eficienţă posibil într-o perioadă plină de provocări și că sumele cuprinse în bugetul instituției au făcut obiectul unei atente administrări.