AUTORITATEA NAŢIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

R A P O R T A N U A L

2020

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

Stimată Doamnă Preşedinte al Senatului,

Stimaţi Senatori,

Anul 2020 a constituit o perioadă de consolidare a respectării 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.

În contextul particularităților generate de evoluția pandemiei de Covid-19, au continuat eforturile operatorilor din mediul public și privat de aplicare a regulilor de utilizare a datelor personale, concretizate în special în asigurarea informării persoanelor fizice, în respectarea efectivă a drepturilor acestora, în luarea măsurilor necesare pentru asigurarea confidențialității și securității prelucrărilor efectuate, inclusiv în mediul on-line.

Aș dori să remarc faptul că activitatea responsabilului cu protecția datelor a avut un impact favorabil în asigurarea respectării normelor de protecția datelor personale de către operatorii din România și, implicit, efecte benefice în privința respectării drepturilor specifice ale persoanelor fizice.

Raportat la obiectivele instituției noastre de monitorizare și control a modului de respectare a regulilor de prelucrare a datelor personale la nivelul operatorilor din sectorul public și privat, precum și de informare a publicului larg, subliniem că, în anul 2020, au continuat acțiunile de control, demarate din oficiu sau pe baza plângerilor și sesizărilor primite. Aș dori să menționez că plângerile primite din partea persoanelor fizice au avut, în principal, ca obiect dezvăluirea datelor cu caracter personal fără consimțământul persoanelor vizate, încălcarea drepturilor și a principiilor prevăzute de Regulamentul General privind Protecția Datelor, instalarea de sisteme de supraveghere video la nivelul diverselor entități, primirea de mesaje comerciale nesolicitate, încălcarea măsurilor de securitate și confidențialitate a prelucrărilor de date personale.

De asemenea, în cursul anului 2020, Autoritatea naţională de supraveghere a continuat activităţile de comunicare destinate informării publicului larg, cu privire la condițiile specifice de prelucrare a datelor cu caracter personal, adaptate la modalitățile particulare de desfășurare a acestora în contextul evoluțiilor pandemice ce au persistat în cursul anului. Astfel, pe lângă organizarea anuală, în format de videoconferință, de către instituția noastră a evenimentelor prilejuite de Ziua Europeană a Protecției Datelor (pe 28 Ianuarie), au fost intensificate comunicatele de presă care au reflectat măsurile adoptate și punctele de vedere ale instituției noastre.

În același timp, în acest an s-a putut observa menținerea la nivel similar a numărului de solicitări de puncte de vedere, precum și primirea spre avizare a mai multor proiecte de acte normative, ceea ce relevă preocuparea crescută a operatorilor în asigurarea respectării regulilor de prelucrare a datelor personale, instituite de Regulamentul General privind Protecția Datelor și de legislația națională conexă.

În contextul pandemic existent, putem aprecia că obiectivele stabilite pentru anul 2020 au fost îndeplinite, ceea ce reprezintă un real succes în condițiile în care resursele umane și financiare de care am dispus au fost insuficiente.

În perspectivă, pe termen scurt și mediu, în concordanță cu competențele sale legale, Autoritatea națională de supraveghere va urmări continuarea activității de monitorizare și control a operatorilor din sectorul public și privat, prin efectuarea de investigații pe baza plângerilor și sesizărilor primite sau din oficiu, continuarea activităților de informarea publică a persoanelor fizice, operatorilor și mass-mediei, precum și continuarea colaborării cu toate instituțiile și entitățile, inclusiv cu societatea civilă, în vederea asigurării unei corecte aplicări a Regulamentului General privind Protecția Datelor și a celorlalte reglementări specifice acestui domeniu.

Cu acest prilej, permiteți-mi să vă mulțumesc pentru sprijinul acordat instituției noastre și să-mi exprim încrederea că vom beneficia de suportul dumneavoastră în continuare, pentru asigurarea unor standarde adecvate în domeniul protecției datelor cu caracter personal în România.

Ancuţa Gianina OPRE,

Preşedinte

CUPRINS

CAPITOLUL I
PREZENTARE GENERALĂ

Raportul de activitate pe anul 2020 al Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (denumită în continuare Autoritatea naţională de supraveghere) este structurat pe cinci capitole, astfel:

Capitolul I conține o prezentare sintetică a principalelor activități desfășurate care se subsumează competențelor legale și obiectivelor Autorității naționale de supraveghere. În concordanță cu reglementările specifice domeniului protecției datelor cu caracter personal, întreaga activitate a instituției urmărește atingerea obiectivelor principale care constau în monitorizarea și controlul aplicării regulilor de prelucrare a datelor personale, în consilierea legislativă a autorităților publice competente, în promovarea acțiunilor de informare a publicului larg și în asigurarea cooperării pe plan european și internațional.

În acest sens, reliefăm că, în cadrul **Capitolului al II-lea,** sunt cuprinse informații sintetice și relevante referitoare la activitatea de reglementare, de avizare a proiectelor de acte normative, la cea de autorizare şi de consiliere, precum şi la aceea de informare publică, în conformitate cu sarcinile și competențele stabilite de Regulamentul (UE) 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul General privind Protecția Datelor), denumit în continuare Regulamentul (UE) 679/2016.

Această activitate s-a concretizat în emiterea de avize asupra unui număr însemnat de proiecte de acte normative şi în elaborarea de puncte de vedere referitoare la aplicarea adecvată a Regulamentului (UE) 679/2016 și a celorlalte reglementări incidente. Acestea s-au subsumat obiectivului de informare a publicului larg și de consiliere legislativă oferită autorităților sau instituțiilor publice competente, în conformitate cu Regulamentul (UE) 679/2016.

În contextul punerii efective în aplicare a Regulamentului (UE) 679/2016 începând din 25 mai 2018, subliniem că, în anul 2020, 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 acestora în diferite situații concrete.

În secţiunea privind reprezentarea în faţa instanţelor de judecată, sunt ilustrate cele mai semnificative litigii finalizate pe parcursul anului 2020, în care a fost parte Autoritatea naţională de supraveghere, cu evidenţierea soluţiilor definitive pronunţate.

Secţiunea privind informarea publică expune principalele modalităţi de popularizare a Regulamentului (UE) 679/2016 în cursul anului 2020, 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 monitorizare și control a Autorității naționale de supraveghere, în privinţa investigaţiilor din oficiu şi a celor efectuate pe baza plângerilor ori sesizărilor primite, conținând și date 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) 679/2016, precum și ca urmare a sesizărilor transmise Autorității naționale de supraveghere.

În ceea ce privește incidentele de securitate, reliefăm faptul că acestea au vizat, în principal, următoarele aspecte: confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare a dezvăluirilor neautorizate ori ca urmare a unui software malițios (ransomware), accesul ilegal la datele cu caracter personal ale clienților din sistemul bancar, accesul neautorizat la sistemele de supraveghere video cu circuit închis (CCTV), dezvăluiri de date cu caracter personal.

În ceea ce privește soluționarea plângerilor și a sesizărilor, în anul 2020 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 capitolului al III - lea sunt evidențiate măsurile corective dispuse în urma investigațiilor efectuate, inclusiv sancțiunile cu avertisment și amendă stabilite, dar și o serie de exemple în care au fost prezentate aspectele investigate.

În cadrul investigaţiilor efectuate în anul 2020, au fost aplicate sancţiuni contravenţionale constând în amenzi în cuantum total de 892.115,95 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 având în vedere resursele umane și financiare insuficiente.

CAPITOLUL II

ACTIVITATEA DE REGLEMENTARE, AVIZARE, CONSULTARE ŞI INFORMARE PUBLICĂ

Secțiunea 1
Activitatea de reglementare a Autorității naționale de supraveghere

Proiectul de Decizie a Preşedintelui Autorității naționale de supraveghere privind „Cerințele suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679”

Regulamentul (UE) 2016/679 prevede că statele membre, autoritățile naționale de supraveghere, Comitetul European pentru 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.

Corelat cu aceste prevederi, 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.

În acest context, încă din anul 2019, la nivelul Autorității naționale de supraveghere a fost elaborat, proiectul deciziei cu caracter normativ privind „Cerințe suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679” .

La întocmirea proiectului au fost luate în considerare o serie de documente, printre care și cerințele EN-ISO/IEC 17065/2012 și Ghidul nr. 1/2018 privind certificarea și

identificarea criteriilor de certificare, respectiv Ghidul nr. 4/2019 privind acreditarea organismelor de certificare în temeiul articolului 43 din Regulamentul (UE) 2016/679, adoptate de Comitetul european pentru protecția datelor.

În luna ianuarie 2020**,** proiectul documentului „Cerințe suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679" a fost supus atenției Asociației de Acreditare din România – RENAR, în vederea formulării de observații și propuneri, în considerarea calității oficiale a RENAR de organism național de acreditare, în temeiul Regulamentului (CE) nr. 765/2008, al O.G. nr. 23/2009 și al Legii nr. 190/2018.

Asociația de Acreditare din România – RENAR a formulat propuneri și observații cu privire la documentul menționat, acestea fiind analizate la nivelul Autorității naționale de supraveghere. În luna iulie 2020 a avut loc o întâlnire între reprezentanții RENAR și cei ai Autorității naționale de supraveghere, iar ulterior proiectul documentului a fost modificat și supus din nou atenției RENAR.

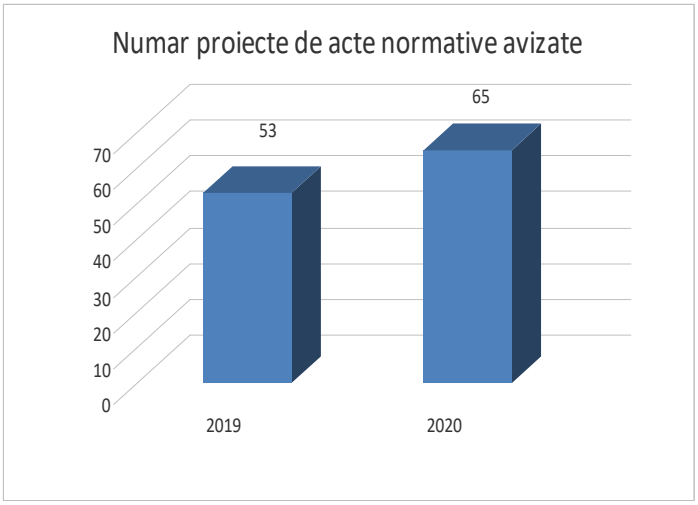
În data de 10.09.2020, Autoritatea națională de supraveghere a publicat pe site-ul www.dataprotection.ro, proiectul de Decizie a Autorității naționale de supraveghere privind Cerințele suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679, supus dezbaterii publice în conformitate cu dispozițiile Legii nr. 52/2003 privind transparența decizională în administrația publică, republicată.

Ca urmare a postării pe site-ul Autorității naționale de supraveghere a Proiectului de Decizie a Preşedintelui Autorității naționale de supraveghere privind „Cerințele suplimentare pentru acreditarea organismelor de certificare în temeiul art. 43 din Regulamentul (UE) 2016/679", au fost primite observații și propuneri de la: Certinspect Register SRL, ASCPD Romania, AmChamRomania, Consiliul Investitorilor Străini – FIC.

Propunerile și observațiile au fost analizate la nivelul instituției noastre, însă nu au fost reținute elemente care să necesite modificarea sau completarea proiectului de Decizie. În același timp, documentul a fost transmis către Comitetul European pentru Protecția Datelor, în vederea obținerii avizului acestui for european, în concordanță cu dispozițiile art. 64 din Regulamentul (UE) 2016/679.

Secțiunea a 2-a: Avizarea actelor normative

În anul 2020, Autoritatea naţională de supraveghere a emis avize asupra unui număr de **65 de proiecte de acte normative** elaborate de instituţii şi autorităţi publice care implicau aspecte complexe privind prelucrarea datelor cu caracter personal, în concordanță cu atribuțiile stabilite prin prevederile 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 Protecției Sociale, Ministerul Lucrărilor Publice, Dezvoltării și Administrației, Ministerul Agriculturii și Dezvoltării Rurale, Ministerul Transporturilor, Infrastructurii și Comunicațiilor, Ministerul Finanțelor Publice, Ministerul Justiției, Ministerul Mediului, Apelor și Pădurilor, Ministerul Afacerilor Externe, Ministerul Educației și Cercetării, dar și de către alte autorități sau instituții publice centrale, cum ar fi: Autoritatea Electorală Permanentă, Centrul Național de Răspuns la Incidente de Securitate Cibernetică, Institutul Naţional de Statistică, Autoritatea pentru Digitalizarea României, Casa Națională de Asigurări de Sănătate.

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

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

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

► **Ministerul Transporturilor, Infrastructurii și Comunicațiilor a transmis Autorității naționale de supraveghere *proiectul de Lege pentru modificarea și completarea unor acte normative în domeniul comunicațiilor electronice și pentru stabilirea unor măsuri de facilitare a dezvoltării rețelelor de comunicații electronice.***

Faţă de prevederile proiectului menționat anterior, care asigură transpunerea în legislația națională a Directivei (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicaţiilor electronice, Autoritatea națională de supraveghere a formulat, în principal, următoarele observații:

În legătură cu obținerea de către ANCOM a informațiilor și datelor înregistrate în registrul comerțului computerizat deținut de Oficiul Național al Registrului Comerțului, precum și a informațiilor deținute de Ministerul Finanțelor Publice și Agenția Națională de Administrare Fiscală, inclusiv prin accesul la sistemele informatice ale acestor instituții, ca urmare a încheierii unor protocoale, s-a subliniat că, în ceea ce privește modalitatea de prelucrare a datelor cu caracter personal, potrivit Regulamentului (UE) 2016/679, aceasta se realizează cu consimțământul persoanei vizate sau în celelalte condiții, prevăzute de art. 6, art. 9 și art. 10, în funcție de natura datelor și categoriilor de date colectate și prelucrate (dezvăluite).

În acest context, s-a precizat că, așa cum a statuat și Curtea de Justiție a Uniunii Europene în cauza C-201/14, în ceea ce privește baza legală a transmiterii unor date personale între diverse entități publice,”modalităţile de efectuare a transmiterii acestor informaţii 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.”.

Totodată, Curtea de Justiție a Uniunii Europene a reținut că ”În aceste împrejurări, nu se poate considera că sunt îndeplinite condițiile prevăzute la articolul 13 din Directiva 95/46 pentru ca un stat membru să poată deroga de la drepturile și obligațiile care decurg din articolul 10 din această directivă.”.

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

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

Referitor la informarea persoanei vizate, art. 12 din Regulamentul (UE) 2016/679 prevede că operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informaţii menţionate la articolele 13 şi 14 şi orice comunicări în temeiul articolelor 15-22 şi 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil.

Prin urmare, pentru asigurarea principiului transparenței, informarea se realizează în funcție de circumstanțele prelucrării datelor obținute direct sau indirect de către operatori (în speță, ANCOM, Oficiul Național al Registrului Comerțului, Ministerul Finanțelor Publice și Agenția Națională de Administrare Fiscală), în modalitățile prevăzute de lege, prezentate mai sus.

În ceea ce privește punctul 30 al art. 5 din proiectul de lege referitor la modificarea art. 18 alin. (1) din Ordonanța de urgență a Guvernului nr. 34/2008 privind organizarea și funcționarea Sistemului național unic pentru apeluri de urgență - SNUAU, prin care ”furnizorii de servicii de comunicații interpersonale bazate pe numere, destinate publicului, au obligația de a pune la dispoziția administratorului SNUAU și de a actualiza, până la data de 25 a fiecărei luni, în mod gratuit, în formatul stabilit de Autoritatea

Națională pentru Administrare și Reglementare în Comunicații, bazele de date proprii care conțin numerele de telefon, identificatorul unic transmis către SNUAU la momentul apelării Serviciului de urgență 112 pentru fiecare utilizator final al serviciului, numele, prenumele, domiciliul, denumirea și sediul social al utilizatorilor finali, codul numeric personal, informații cu privire la serviciul furnizat și mobilitatea utilizatorului, precum și numele ori denumirea furnizorului de servicii de comunicații electronice destinate publicului", s-a apreciat că trebuie pus în acord cu principiul "reducerii la minimum a datelor" potrivit căruia datele sunt adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (în speță, dezvăluite) - art. 5 din Regulamentul (UE) 679/2016.

Prin urmare, Autoritatea națională de supraveghere a considerat că prevederile menționate din proiectul de Cod al comunicațiilor trebuie reanalizate prin raportare la aspectele prezentate.

► **Ministerul Lucrărilor Publice, Dezvoltării și Administrației a solicitat un punct de vedere referitor la *proiectul de Hotărâre a Guvernului privind procedura de desemnare, atribuțiile, modalitatea de organizare a activității și procedura de evaluare a performanțelor profesionale individuale ale funcționarului public desemnat consilier de etică, precum și pentru aprobarea modalității de raportare a instituțiilor și autorităților în scopul asigurării implementării, monitorizării și controlului respectării principiilor și normelor privind conduita funcționarilor publici.***

Autoritatea națională de supraveghere a recomandat introducerea unui articol distinct în textul Hotărârii în care să se menționeze că orice activitate care implică prelucrarea datelor cu caracter personal, realizată în aplicarea dispoziţiilor referitoare la desemnarea, atribuțiile, modalitatea de organizare a activității și procedura de evaluare a performanțelor profesionale individuale ale funcționarului public desemnat consilier de etică, precum și în legătură cu celelalte activități ale instituțiilor și autorităților realizate în scopul asigurării implementării, monitorizării și controlului respectării principiilor și normelor privind conduita funcționarilor publici, se efectuează cu respectarea

prevederilor Regulamentului (UE) 2016/679, inclusiv în ceea ce privește confidențialitatea și securitatea prelucrărilor.

De asemenea, Autoritatea națională de supraveghere a solicitat reanalizarea conținutului Anexei 1 – *"Declarație de integritate"* din proiectul de Hotărâre și eliminarea referirilor la obținerea consimțământului persoanei vizate (funcționarul public care manifestă opțiunea individuală de a dobândi calitatea de consilier de etică) cu privire la prelucrarea datelor sale cu caracter personal întrucât prelucrarea datelor personale ale funcționarului public respectiv se efectuează în contextul necesității îndeplinirii unor obligaţii legale ce îi revine operatorului, potrivit art. 6 alin. (1) lit. c) din Regulamentul (UE) 2016/679. Totodată, s-a recomandat completarea anexei conform dispozițiilor art. 13 din Regulamentul (UE) 2016/679 referitoare la informarea persoanelor vizate.

Ulterior, Ministerul Lucrărilor Publice, Dezvoltării și Administrației a retransmis proiectul de act normativ, modificat conform cerințelor Autorității naționale de supraveghere.

► **Ministerul Afacerilor Interne – Inspectoratul General al Poliției Române a transmis în vederea avizării *proiectul de "Dispoziția Inspectorului General al Inspectoratului General al Poliției Române privind stabilirea regulilor de utilizare a înregistratoarelor audio-video portabile de tip Body Worn Camera"***

Față de textul proiectului, au fost făcute următoarele observații:

a) În preambulul Dispoziției este necesar să se introducă o referire la Legea 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, act normativ ce reglementează prelucrarea datelor cu caracter personal, inclusiv cele efectuate de Poliția Română prin intermediul înregistratoarelor audio-video portabile de tip Body Worn Camera.

Referitor la alt articol, s-a considerat că este necesară completarea acestuia în sensul specificării faptului că doar pentru înregistratoarele audio-video portabile de tip

Body Worn Camera utilizate de polițiști în spațiul public nu este necesar consimțământul persoanelor vizate.

De asemenea, s-a considerat că este necesară introducerea unui nou alineat referitor la informarea persoanelor vizate prin intermediul site-ului Poliției Române cu privire la prelucrarea datelor prin intermediul înregistratoarelor de tip Body Worn Camera portabile, în conformitate cu dispozițiile Legii nr. 363/2018.

În acelasi timp, s-a considerat că textul acestuia ar trebui să fie completat astfel încât să conțină prevederile aplicabile exercitării drepturilor persoanelor vizate, în special modalitatea de exercitare efectivă a acestora, cu excepțiile aferente, în concordanță cu Legea nr. 363/2018.

Cu acest prilej, în contextul implementării prevederilor Legii nr. 363/2018 de către Ministerul Afacerilor Interne, împreună cu structurile aflate în subordinea acestuia (precum Inspectoratul General al Poliției Române), Autoritatea națională de supraveghere a recomandat reanalizarea, modificarea sau completarea și a celorlalte dispoziții, a ordinelor și, după caz, a procedurilor care conțin prevederi referitoare la prelucrări de date cu caracter personal și transmiterea acestora către Autoritatea națională de supraveghere, în vederea avizării, potrivit reglementărilor aplicabile.

Inspectoratul General al Poliției Române a retransmis proiectul de dispoziție și, întrucât au fost preluate observațiile și propunerile Autorității naţionale de supraveghere, s-a comunicat Inspectoratului General al Poliției Române că nu mai sunt alte observații față de conținutul documentului transmis.

► **Ministerul Afacerilor Interne a solicitat un punct de vedere privind *propunerile Ministerului Justiției pentru cel de-al doilea Decret al Președintelui României privind instituirea stării de urgență pe teritoriul României.***

Autoritatea națională de supraveghere a formulat următoarele observații și propuneri:

Raportat la prevederile din ‟CAPITOLUL III. Domeniul sănătății”, punctul 3 din propunere s-a subliniat că prelucrările de date preconizate a fi efectuate de personalul din sistemul poliției penitenciare, în contextul descris, intră sub incidența Regulamentului

(UE) 2016/679, în principal a dispozițiilor art. 9 alin. (2) lit. i), care stabilește că datele privind starea de sănătate pot fi prelucrate de un operator atunci când *"prelucrarea este necesară din motive de interes public în domeniul sănătăţii publice, cum ar fi protecţia împotriva ameninţărilor transfrontaliere grave la adresa sănătăţii sau asigurarea de standarde ridicate de calitate şi siguranţă a asistenţei medicale şi a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor persoanei vizate, în special a secretului profesional".*

Așadar, personalul din sistemul poliției penitenciare își poate desfășura activitatea, ca și personalul din sistemul sanitar, gestionat de Ministerul Sănătății sau Ministerul Apărării Naționale, în special în temeiul prevederilor art. 6 alin. (2) lit. c), d) și e), precum și art. 9 alin. (2) lit. i) din Regulamentul (UE) 2016/679, cu respectarea, totodată, a celorlalte obligații prevăzute de Regulament, inclusiv cele cu privire la asigurarea securității prelucrărilor și confidențialității datelor.

În caz contrar, efect al normei propuse de Ministerul Justiției, de introducere a unei excepții totale de la respectarea și aplicarea legislației în domeniul protecției datelor cu caracter personal, s-ar ajunge la o încălcare gravă a confidențialității datelor persoanelor implicate, inclusiv la posibile dezvăluiri neautorizate ale datelor privind starea de sănătate. Aceasta echivalează cu încălcarea flagrantă a Regulamentului (UE) 2016/679 și cu nerespectarea dreptului persoanelor vizate la protecția datelor și la viață privată.

Pe de altă parte, s-a menționat că în contextul prelucrărilor precizate, nu pot fi aplicate anumite restricții decât conform art. 23 alin. (1) lit. e) din Regulamentul (UE) 2016/679, cu respectarea art. 6 alin. (3) din Regulament.

Ca atare, Autoritatea națională de supraveghere nu a avizat propunerea de la punctul 3 și a semnalat că norma propusă constituie o gravă încălcare a dispozițiilor Regulamentului (UE) 2016/679 și ale Directivei (UE) 2016/680 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, precum și a legislației naționale dată în aplicarea celor două acte normative comunitare (Legea nr. 190/2018 privind

măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), respectiv Legea 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).

Autoritatea națională de supraveghere a subliniat că întreg sistemul sanitar din România își desfășoară activitățile specifice de îngrijire a pacienților bolnavi cu Covid 19 cu respectarea Regulamentului (UE) 2016/679, în condițiile în care legislația din domeniul protecției datelor nu reprezintă un impediment în desfășurarea activităților în domeniul sanitar, în contextul situației de urgență din România.

În acest context, s-a subliniat faptul că Autoritatea națională de supraveghere și-a exprimat punctul de vedere în data de 18.03.2020, în comunicatul publicat pe site-ul www.dataprotection.ro, pe același site fiind postată și declarația din 16.03.2020 a președintelui Comitetului european pentru protecția datelor, accesibilă și la următorul link: https://edpb.europa.eu/news/news_ro.

► **Institutul Național de Statistică a transmis spre analiză *proiectul de Hotărâre a Guvernului privind bugetul și categoriile de cheltuieli pentru recensământul populației și locuințelor din România în anul 2021 precum și stabilirea măsurilor privind implementarea unor dispoziții ale Ordonanței de urgență a Guvernului nr. 19/2020***.

Având în vedere conținutul proiectului supus atenției Autorității naționale de supraveghere, au fost formulate observații și propuneri cu privire la Anexa nr. 4 din proiectul de Hotărâre care conține modelul Contractului cadru de servicii pentru recensământul populației și locuințelor din anul 2021.

Cu referire la obligația respectării confidențialității tuturor datelor culese pe întregul circuit al prestării de servicii de culegere de date statistice de către personalul de

recensământ, așa cum este prevăzută la alin. (1) al art. 4 – ”Obligațiile personalului de recensământ” din modelul de contract, s-a considerat că este necesar ca angajamentul privind păstrarea confidențialității datelor să devină anexă la contractul cadru și să cuprindă inclusiv referiri la instruirea personalului de recensământ cu privire la modul în care acesta asigură confidențialitatea datelor prelucrate în cadrul serviciilor prestate.

Totodată, raportat la prevederile art. 27 din OUG nr. 19/2020, s-a subliniat că este necesară introducerea unui nou articol în cuprinsul modelului de Contract cadru prin care să se prevadă că Institutul Național de Statistică, direcțiile sale teritoriale, precum și unitățile administrativ teritoriale, în calitate de operatori de date cu caracter personal, răspund pentru prelucrările efectuate, în conformitate cu Regulamentul (UE) 679/2016.

► **Autoritatea Electorală Permanentă a transmis *proiectul de hotărâre a Autorităţii Electorale Permanente pentru aprobarea procedurii de acreditare, a modelelor documentelor de acreditare și a modelelor ecusoanelor persoanelor acreditate la alegerile pentru autoritățile administrației publice locale din anul 2020.***

În urma analizării acestui proiect, raportat la stabilirea transmiterii documentelor către Autoritatea Electorală Permanentă prin fax sau e-mail, în contextul alegerilor, Autoritatea națională de supraveghere a subliniat necesitatea respectării, la alegerea mijloacelor de prelucrare, a art. 24 coroborat cu art. 32 din Regulamentul (UE) 679/2016, ce impun luarea de măsuri tehnice şi organizatorice adecvate de către operatorul de date, în vederea asigurării unui nivel de securitate corespunzător riscurilor pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu Regulamentul.

► **Institutul Național de Statistică a solicitat avizul asupra *proiectului de Ordonanță de urgență privind organizarea și desfășurarea Recensământului Populației și Locuințelor din România în anul 2021.***

Față de textul proiectului actului normativ sus-menționat, având în vedere că activităţile desfăşurate în contextul reglementării domeniului recensământului presupun efectuarea de operaţiuni de prelucrare a unor categorii diferite de date cu caracter

personal, printre care şi date cu caracter special, cu implicaţii asupra drepturilor fundamentale ale persoanelor fizice, putând conduce la atingeri aduse dreptului la viaţă privată, Autoritatea națională de supraveghere a avizat cu observații proiectul de ordonanță de urgență.

Astfel, la art. 19 lit. i) din proiect, s-au făcut observații în ceea ce privește confidențialitatea și luarea de măsuri tehnice și organizatorice pentru stocarea datelor în condiții de siguranță, limitarea accesului la datele colectate doar la persoanele autorizate în acest sens, instruirea personalului implicat.

În ceea ce privește drepturile persoanelor vizate, s-a subliniat faptul că la art. 26 alin. (3) din proiect se precizează faptul că art. 15, 16, 18 și 21 din Regulamentul (UE) 679/2016 nu se aplică, dar cu toate acestea nu se fac mențiuni despre menținerea celorlalte drepturi prevăzute de Regulamentul (UE) 679/2016, pentru care nu sunt prevăzute derogări, precum și modalitatea lor de exercitare, inclusiv sub aspectul adresării cererilor persoanelor vizate, textul fiind în contradicție cu art. 89 alin. (2) din Regulamentul (UE) 679/2016 și art. 8 din Legea nr. 190/2018.

Prin urmare, în considerarea asigurării garanțiilor corespunzătoare protejării drepturilor persoanelor vizate, s-a evidențiat că este necesară realizarea unei distincții referitoare la exercitarea drepturilor garantate de Regulamentul (UE) 679/2016.

De asemenea, s-a arătat că la art. 25 alin. (3) din proiect se prevede faptul că toate întrebările incluse în formulare au caracter obligatoriu. În acest sens, s-a subliniat că textul anterior nemodificat al art. 25 alin. (3), care excepta furnizarea datelor privind etnia, limba maternă și religia, asigura garanțiile corespunzătoare drepturilor și libertăților persoanelor fizice. Pentru aceste motive s-a solicitat reanalizarea textului și stabilirea unei distincții între datele obligatorii și cele facultative, raportat și la faptul că pentru acestea din urmă drepturile prevăzute la art. 15, 16, 18 și 21 din Regulamentul (UE) 679/2016 se aplică.

În același timp, raportat la volumul datelor prelucrate, Autoritatea națională de supraveghere a considerat faptul că textul nu este în acord cu principiul minimizării datelor prevăzut de art. 5 coroborat cu art. 89 din Regulamentul (UE) 679/2016, respectiv datele strict necesare îndeplinirii scopului legii de față, fiind de domeniul legii statisticii oficiale.

Prin urmare, Autoritatea națională de supraveghere a solicitat reanalizarea art. 28 din proiect în vederea respectării principiilor privind prelucrarea și protecția datelor, precum și instituirea de garanții în concordanță cu art. 89 alin. (2) din Regulamentul (UE) 2016/679.

► **Ministerul Educației și Cercetării a solicitat exprimarea unui punct de vedere cu privire la *proiectul Ordonanței de urgență a Guvernului privind luarea unor măsuri pentru buna funcționare a sistemului de învățământ și pentru modificarea și completarea Legii educației naționale nr. 1/2011*.**

Faţă de textul proiectului sus-menționat, au fost aduse în atenția acestui minister următoarele aspecte:

Referitor la sintagma generică ”prin intermediul tehnologiei și a internetului” utilizată la art. 3 alin. (1) din proiect, raportat la principiul responsabilității operatorului statuat de art. 5 alin. (1) lit. f) coroborat cu art. 24 din Regulamentul (UE) 679/2016, precum și pentru respectarea principiilor predictibilității și previzibilității actelor normative și evitarea unei aplicări neunitare în practică, s-a arătat că este necesară stabilirea concretă, prin lege, a modalității de desfășurare a activității didactice cu ajutorul noilor tehnologii. În acest sens, spre exemplu, s-a evidențiat faptul că la art. 8 alin. (2) din proiect se specifică modalitatea de raportare de către cadrele didactice universitare a activității desfășurate prin intermediul platformelor on-line.

La art. 4 din proiect, unde se precizează faptul că va fi elaborată o metodologie - cadru de către Ministerul Educației și Cercetării, ce va fi aprobată prin ordin al ministrului, s-a subliniat faptul că la elaborarea acestei metodologii, având în vedere obiectul de reglementare, este necesară acordarea unei atenții sporite asigurării securității datelor cu caracter personal.

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

Art. 5 alin. (1) lit. (f) din același Regulament stabilește unul dintre principiile potrivit căruia datele trebuie prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate").

De asemenea, art. 24 din Regulamentul (UE) 679/2016 stabilește ca responsabilitate a operatorului punerea în aplicare de măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu acest Regulament.

Totodată, art. 25 din Regulamentul (UE) 679/2016 stabilește asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit, respectiv asigurarea principiilor privacy by design și by default.

Față de dispozițiile legale de mai sus și având în vedere faptul că se prelucrează date cu caracter personal aparținând grupurilor vulnerabile – minorii - care necesită o protecție sporită, raportat la dispozițiile art. 10 lit. e) din Legea nr. 102/2005, republicată, Autoritatea națională de supraveghere a solicitat transmiterea, spre avizare, și a proiectului metodologiei prevăzute la art. 4 din proiectul ordonanței de urgență.

► **Ministerul Educației și Cercetării a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la *proiectul Memorandum-ului pe tema utilizării datelor și informațiilor existente în bazele de date de la nivelul Ministerului Educației și Cercetării, Ministerului Muncii și Protecției Sociale, Inspecției Muncii, Ministerului de Finanțe și Agenției Naționale de Administrare Fiscală în vederea monitorizării inserției profesionale a absolvenților din învățământul preuniversitar/universitar.***

Față de memorandumul supus analizei, Autoritatea națională de supraveghere a apreciat că prelucrarea datelor nu respectă principiile legalității și proporționalității stabilite de art. 5 prin raportare la art. 6 din Regulamentul (UE) 2016/679, ținând cont de condițiile de legitimitate și principiile prelucrării stabilite de Regulament raportat la scopul prelucrării, respectiv interconectarea bazelor de date gestionate de diferite instituții publice în scopuri total diferite.

De asemenea, instituția noastră a subliniat faptul că instituțiile publice, care dețin sisteme de evidență a datelor personale la nivel național, au cu atât mai mult obligația legală pozitivă de a asigura respectarea drepturilor şi libertăţilor fundamentale ale cetăţenilor aflați pe o poziție de inegalitate, întrucât prelucrarea (dezvăluirea) nu se efectuează pe baza consimțământului lor.

► **Ministerul Muncii și Protecției Sociale a transmis în vederea avizării *proiectul Ordonanței de urgență a Guvernului privind acordarea unor zile libere părinților pentru supravegherea copiilor, în situația suspendării cursurilor sau închiderii temporare a unor unități de învățământ ca urmare a răspândirii coronavirusului SARS – COV – 2.***

Faţă de textul proiectului sus-menționat, au fost efectuate în principal următoarele observațiile și propuneri:

Referitor la mențiunile de la art. 2 alin. (3) din proiect, în considerarea respectării principiului reducerii la minimum a datelor prevăzut de art. 5 alin. (1) lit. c) din Regulamentul (UE) 679/2016, s-a considerat că este necesară reanalizarea obligativității depunerii la angajator, de către părinte, a copiei certificatului de naștere a copilului, în condițiile în care aceasta există deja la dosarul de personal al angajatului.

De asemenea, referitor la mențiunile de la art. 2 alin. (4) și art. 4 alin. (4) din proiect, în considerarea respectării aceluiași principiu, s-a subliniat faptul că la stabilirea, prin ordin de ministru, a modelului cererilor, declarației pe propria răspundere, este necesară luarea în considerare a faptului că trebuie să se colecteze și prelucreze datele adecvate, relevante și limitate la ceea ce este necesar în raport de scopul prelucrării.

La art. 4 alin. (2) din proiect, sintagma ”...se transmit electronic” are o formulare generică și nu indică cu claritate care sunt mijloacele de comunicare electronică a documentelor, respectiv de prelucrare a datelor, raportat la definiția operatorului de date (art. 4 pct. 7 din Regulamentul (UE) 679/2016), potrivit căreia operatorul este cel care stabilește scopul și mijloacele de prelucrare, precum și la principiul responsabilității operatorului și la obligația de asigurare a securității datelor, stabilite de art. 24 și 32 din Regulamentul (UE) 679/2016.

În acest sens, s-a propus reanalizarea textului art. 4 alin. (2) din proiect, în sensul stabilirii unor mijloace de comunicare electronică care să asigure securitatea prelucrării.

Aceleași observații s-au efectuat și cu privire la mențiunile de la art. 5 referitoare la transmiterea listelor nominale cuprinzând elevii. La același articol, s-a subliniat și necesitatea respectării principiului limitării legate de stocare, statuat de art. 5 alin. (1) lit. c) din Regulamentul (UE) 679/2016, respectiv efectuarea de mențiuni privind păstrarea datelor elevilor de către agențiile pentru ocuparea forței de muncă pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. În acest sens, avem în vedere faptul că se urmărește comunicarea fără distincție a listelor nominale ale elevilor unităților de învățământ închise sau ale căror cursuri se suspendă, indiferent dacă părintele a depus sau nu cerere către angajator pentru solicitarea zilelor libere ori nu se încadrează în condițiile stabilite de proiectul de act normativ, motiv pentru care este necesară asigurarea unor garanții pentru protecția datelor personale ale minorilor.

► **Secretariatul General al Guvernului - Departamentul pentru Relația cu Parlamentul a transmis în vederea exprimării opiniei Autorității naționale de supraveghere, *Propunerea legislativă pentru transparentizarea informaţiilor de interes public şi uşurarea accesului cetăţenilor prin modificarea şi completarea Legii nr. 544/2001 privind liberul acces la informaţii de interes public (Bp. 410/2020).***

Faţă de textul propunerii de lege sus-menționate, Autoritatea națională de supraveghere a comunicat faptul că nu susține propunerea de lege în forma transmisă.

Raportat la obiectul propunerii legislative, având în vedere faptul că se urmărește înființarea unui registru electronic privind informațiile de interes public, urmat de publicarea conținutului acestuia pe Internet, s-au precizat următoarele:

Potrivit art. 4 pct. 1 din Regulamentul (UE) 2016/679, "date cu caracter personal" înseamnă orice informaţii privind o persoană fizică identificată sau identificabilă ("persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la

unul sau mai multe elemente specifice, proprii identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale".

Față de definiția mai sus menționată, informațiile referitoare la un număr de identificare sau elemente specifice, proprii identităţii economice, culturale sau sociale reprezintă date cu caracter personal, deoarece pot conduce la identificarea în mod indirect a persoanelor fizice în cauză, solicitanți ai informațiilor de interes public.

Legat de aspectele de mai sus, s-a arătat că registrul electronic în cauză va conține atât solicitările petenților, cât și răspunsurile comunicate, iar publicarea va viza conținutul acestora în integralitate (pct. 1 și 3 din propunere), cu anonimizarea sau înlăturarea datelor personale conținute.

În acest context, raportat la unii termeni utilizați în propunerea legislativă s-a precizat faptul că aceștia nu au corespondent în Regulamentul (UE) 2016/679.

Astfel, art. 4 pct. 5 din Regulamentul (UE) 2016/679 definește "pseudonimizarea" ca fiind "prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile".

Raportat la publicarea pe internet a unor date cu caracter personal (așa cum sunt definite la art. 4 pct. 1 din Regulamentul (UE) 2016/679 mai sus menționat), s-a subliniat faptul că diseminarea în spațiul virtual a datelor persoanelor fizice identificabile și, implicit, punerea la dispoziția unui număr potențial foarte mare de persoane, fără niciun control asupra utilizării ulterioare a datelor în scopuri posibil incompatibile cu scopul inițial, poate reprezenta o ingerință gravă în drepturile la viaţă privată și protecția datelor cu caracter personal, astfel cum sunt garantate de art. 26 din Constituție, art. 8 din Convenţia Europeană a Drepturilor Omului, precum și art. 7 și 8 din Carta Drepturilor Fundamentale a UE.

Raportat la cele de mai sus, publicarea solicitărilor petenților și răspunsurilor aferente în baza Legii nr. 544/2001 pe Internet poate aduce beneficii, însă s-a evidențiat că în cuprinsul acestor documente pot exista o multitudine de informaţii care pot

conduce ulterior la (re)identificarea unei persoane fizice, prin combinarea cu alte informaţii existente în mediul on-line, ceea ce poate determina riscul apariţiei unor situaţii (posibil grave) de încălcare a drepturilor persoanelor fizice.

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

Ca atare, înainte de a stabili, prin lege, publicarea de informații referitoare la o persoană fizică, în aplicarea principiului proporționalității, trebuie să se stabilească măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor persoanei vizate, raportat la datele și categoriile de date ce urmează a fi dezvăluite, mijloacele de prelucrare, operațiunile efectuate asupra datelor, precum și la categoriile de persoane vizate (de ex. apartenența la anumite categorii vulnerabile) care necesită protecție.

De asemenea, s-a precizat faptul că art. 5 din Legea nr. 544/2001, cu modificările și completările ulterioare, instituie deja obligația ca fiecare autoritate sau instituţie publică să comunice din oficiu o serie de informaţii de interes public, să publice şi să actualizeze anual un buletin informativ care va cuprinde aceste informaţii, precum și obligația de a da din oficiu publicităţii un raport periodic de activitate, cel puţin anual, care va fi publicat în Monitorul Oficial al României, Partea a III-a.

Astfel, raportat la obligațiile suplimentare instituite autorităților și instituțiilor publice, în cazul de față a celor ce intră sub incidența Legii nr. 544/2001, s-a subliniat faptul că, în jurisprudența sa, Curtea Europeană a Drepturilor Omului ”acceptă faptul că nu trebuie impusă o sarcină imposibilă sau exorbitantă autorităţilor fără să se ţină seama în special de alegerile pe care acestea trebuie să le facă prin raportare la priorităţi şi resurse” (a se vedea cauza Osman împotriva Regatului Unit, nr. 23.452/94, 28 octombrie 1998, Hajduová împotriva Slovaciei, nr. 2.660/03, cauza Georgel și Georgeta Stoicescu împotriva României, nr. 9.718/03).

Având în vedere aceste prevederi, Autoritatea națională de supraveghere a apreciat că publicarea pe internet în vederea reutilizării informațiilor din documentele aflate în posesia instituţiilor publice pe care acestea din urmă le-au creat în cadrul activităţii publice proprii, după cum se motivează în ”Expunerea de motive” a propunerii legislative, și care în plus conțin date cu caracter personal, intră în contradicție cu prevederile Legii nr. 109/2007 și ale Regulamentului (UE) 2016/679.

► **Ministerul Fondurilor Europene a solicitat exprimarea unui punct de vedere cu privire la *proiectul de Ordonanță de urgență a Guvernului privind unele măsuri pentru sprijinirea categoriilor de persoane cele mai defavorizate care beneficiază de mese calde pe bază de tichete electronice din fonduri externe nerambursabile, precum și unele măsuri de distribuire a acestora.***

Autoritatea națională de supraveghere a formulat o serie de observații și propuneri.

Astfel, în proiect cât și în nota de fundamentare s-a propus înlocuirea sintagmei „protocol” cu aceea de „act administrativ cu caracter normativ”, raportat la necesitatea asigurării transparenței acestui document.

În acest context s-a precizat că, așa cum a statuat și CJUE în Cauza Bara împotriva României C-201/14, în ceea ce privește baza legală a transmiterii unor date personale între diverse entități publice, ”modalităţile de efectuare a transmiterii acestor informaţii 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.”

Totodată, în proiect s-a solicitat eliminarea înscrierii pe tichetul social a „codului numeric personal al destinatarului final eligibil”, raportat la scopul prelucrării, respectiv acordarea de mese calde către persoanele defavorizate, pentru respectarea principiului proporționalității prelucrării de date personale.

În consecinţă, s-a propus ca textul proiectului să se modifice în concordanţă cu observaţiile şi propunerile efectuate de Autoritatea națională de supraveghere.

► **Autoritatea Electorală Permanentă a solicitat exprimarea unui punct de vedere cu privire la *proiectul de hotărâre a Autorității Electorale Permanente privind aprobarea procedurii de monitorizare video a localurilor secțiilor de votare din străinătate la alegerile pentru Senat si Camera Deputatilor*.**

Având în vedere textul proiectului, s-a atras atenția asupra faptului că este necesară introducerea unui articol în care să se menționeze că toate entitățile implicate în prelucrarea datelor cu caracter personal au obligația să respecte prevederile Regulamentului (UE) 2016/679, inclusiv în ceea ce privește confidențialitatea și securitatea prelucrărilor.

În același timp, referitor la procedura propusă, s-a apreciat ca fiind necesară completarea acesteia prin raportare la prevederile art. 12 și 13 din Regulamentul (UE) 679/2016, referitoare la asigurarea transparenței prelucrării, în cazul colectării datelor de la persoana vizată.

► **Casa Națională de Asigurări de Sănătate a transmis *proiectul de ordin al ministrului sănătății și al președintelui CNAS pentru aprobarea normelor metodologice pentru implementarea dispozițiilor Legii nr. 165/2019 pentru completarea art. 234 din Legea nr. 95/2006 privind reforma în domeniul sănătății.***

Faţă de conținutul proiectului Autoritatea națională de supraveghere a formulat următoarele observații:

S-a solicitat modificarea art. 3 alin. (3) din Normele metodologice, în sensul eliminării obligativității depunerii copiei actului de identitate al persoanei asigurate, respectiv a reprezentantului legal, raportat la scopul prelucrării de furnizare a listei serviciilor, medicamentelor si dispozitivelor medicale, pentru respectarea principiului proporționalității prelucrării de date personale. Corelat, și în cuprinsul cererii de la Anexa 1 a Normelor, s-a solicitat eliminarea referirii la atașarea copiei actelor de identitate.

De asemenea, în ceea ce privește conținutul cererii (Anexa 1 din Norme), s-a menționat că sintagma „îmi asum răspunderea pentru riscul ca acestea să ajungă la persoane neîndreptățite în cazul transmiterii lor prin poștă/e-mail/fax”, trebuie eliminată,

având în vedere prevederile art. 24 din Regulamentul (UE) 2016/679 care stabilește în sarcina operatorului (CNAS) obligația de a aplica măsuri de securitate și confidențialitate a prelucrărilor.

În același timp, instituția noastră a subliniat că pct. 4 din cuprinsul cererii (Anexa 1 la Norme) trebuie reformulat astfel încât să fie furnizate de CNAS, în calitate de operator de date, persoanelor vizate informaţiile menţionate la articolele 13 şi 14 din Regulamentul (UE) 2016/679.

Prin urmare, Autoritatea națională de supraveghere a recomandat modificarea proiectului *de ordin al ministrului sănătății și al președintelui CNAS pentru aprobarea normelor metodologice pentru implementarea dispozițiilor Legii nr. 165/2019 pentru completarea art. 234 din Legea nr. 95/2006 privind reforma în domeniul sănătății,* în concordanță cu aspectele semnalate.

► **Inspectoratul General al Poliției de Frontieră a transmis *proiectul Legii privind operaționalizarea și gestionarea la nivel național a Sistemului de intrare/ieșire (EES) și a Sistemului european de informații și de autorizare privind călătoriile (ETIAS), precum și de completare a art. 3^1 alin. (3) din Ordonanța de urgență a Guvernului nr. 104/2001 privind organizarea și funcționarea Poliției de Frontieră Române.***

Faţă de conținutul proiectului instituția noastră a formulat următoarele observații:

S-a propus introducerea unui alineat nou după alin. (2) al aceluiași articol, raportat la prevederile art. 55 alin. (4) din Regulamentul EES și art. 66 alin. (6) din Regulamentul ETIAS, cu următorul conținut:

„Autoritățile naționale competente desemnate prin art. 5 din prezenta lege furnizează toate informațiile solicitate de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, acordă acesteia accesul la evidențele lor și îi permit în orice moment accesul la toate incintele lor utilizate în scopul ETIAS/EES.”

Totodată, Autoritatea națională de supraveghere a solicitat reformularea alineatului (4) al art. 13 prin raportare la art. 52 alin. (4) din Regulamentul (UE) 2016/679, astfel:

„(4) Pentru realizarea atribuțiilor prevăzute la art. 55 din Regulamentul EES și art. 66 din Regulamentul ETIAS, inclusiv pentru auditarea EES și ETIAS, se alocă suplimentar Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal 5 posturi,

iar sumele și resursele necesare se suportă de la bugetul de stat și sunt prevăzute distinct anual, cu această destinație, în bugetul Autorității naționale de supraveghere."

În ceea ce privește art. 16 alin. (1) din proiectul de lege, raportat la art. 60 din Legea nr. 363/2018, s-a solicitat reformularea acestuia, astfel:

„(1) În aplicarea art. 45 din Regulamentul EES și a art. 63 din Regulamentul ETIAS, orice persoană care a suferit prejudicii materiale sau morale ca urmare a unei operațiuni ilegale de prelucrare sau a oricărei acțiuni realizată de o autoritate competentă desemnată potrivit art. 5 alin. (1) din prezenta lege, are dreptul de a se adresa instanței de contencios administrativ, competente."

De asemenea, întrucât la alin. (2) al aceluiași articol nu se face referire la Regulamentul (UE) 2016/679 și la Legea nr. 102/2005, republicată, instituția noastră a propus modificarea acestuia astfel:

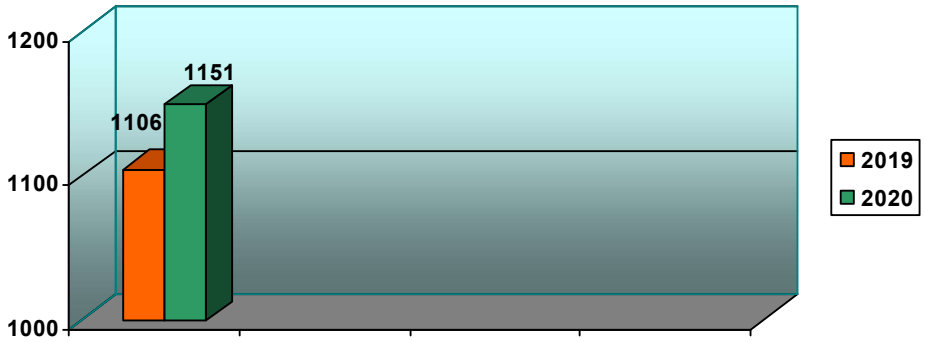
"(2) Utilizarea abuzivă a datelor din EES și ETIAS, prelucrarea acestora sau schimbul de informații care contravine Regulamentelor EES și ETIAS, constatate ca urmare a investigărilor desfășurate de către personalul Autorității naționale de supraveghere cu atribuții în acest scop, se vor sancționa cu măsuri corective și sancțiuni, potrivit reglementărilor legale aplicabile."

Prin urmare, Autoritatea națională de supraveghere a solicitat reanalizarea și modificarea proiectului Legii privind operaționalizarea și gestionarea la nivel național a Sistemului de intrare/ieșire (EES) și a Sistemului european de informații și de autorizare privind călătoriile (ETIAS), precum și de completare a art. 3^1 alin. (3) din Ordonanța de urgență a Guvernului nr. 104/2001 privind organizarea și funcționarea Poliției de Frontieră Române, raportat la observațiile formulate.

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

Pe parcursul anului 2020 a fost adresat Autorității naţionale de supraveghere un număr de **1151** solicitări de emitere puncte de vedere privind diverse aspecte referitoare la modalitatea de interpretare și aplicare a Regulamentului (UE) 679/2016, de către operatori și împuterniciții acestora, din domeniul public și privat, de către alte entități, precum și de către persoane fizice.

Față de anul 2019, când au fost emise **1106** puncte de vedere, în acest an se poate observa menținerea numărului de solicitări la un nivel semnificativ, ceea ce ilustrează un interes real în asigurarea respectării regulilor de prelucrare a datelor personale instituite de Regulamentul (UE) 679/2016 și legislația națională conexă.



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

► ***Prelucrarea datelor minorilor, inclusiv a codului numeric personal, în contextul funcționării sistemului e-ticheting cu carduri***

O societate de transport local a solicitat opinia Autorității naționale de supraveghere cu privire la legalitatea prelucrării datelor minorilor, inclusiv a codului numeric personal, în contextul funcționării „sistemului e-ticheting cu carduri".

Referitor la legitimitatea prelucrării datelor care nu au un caracter special (cum este și codul numeric personal), Autoritatea națională de supravegere a precizat că art. 6 din Regulamentul (UE) 2016/679 stabilește mai multe situații, una dintre acestea fiind cea în care prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului.

În ceea ce privește prelucrarea unui număr de identificare naţional (printre care codul numeric personal, seria şi numărul actului de identitate), inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, art. 4 din Legea nr. 190/2018 prevede următoarele:

„(1) Prelucrarea unui număr de identificare naţional, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conţin, se poate efectua în situaţiile prevăzute de art. 6 alin. (1) din Regulamentul general privind protecţia datelor."

Astfel, s-a precizat că în contextul prelucrării datelor personale, este necesară analizarea temeiului legal al efectuării acesteia, în conformitate cu dispozițiile Regulamentului (UE) 2016/679 și ale Legii nr. 190/2018, mai sus precizate. În acest sens, în măsura în care operatorul identifică faptul că prelucrarea este necesară pentru îndeplinirea unei obligații legale (cum este, în speță, un act normativ al autorității administrației publice locale), datele pot fi prelucrate fără consimțământul persoanei vizate.

Sub aspectul informării persoanelor vizate (indiferent de temeiul prelucrării, la consimțământ sau pe baza altor temeiuri legale), s-a menționat că art. 12 din Regulamentul (UE) 2016/679 prevede că operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informaţii menţionate la articolele 13 şi 14 şi orice comunicări în temeiul articolelor 15-22 şi 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu.

Prin urmare, având în vedere natura datelor prelucrate de către operator (în speță, CNP – ul, datele personale ale minorilor), Autoritatea națională de supraveghere a precizat că este necesară respectarea obligaţiilor stabilite de prevederile legale din Regulamentul (UE) 2016/679 enunțate mai sus, în special a măsurilor privind confidenţialitatea și securitatea datelor.

În ceea ce privește stabilirea necesității prelucrării datelor minorilor, printr-un act normativ al autorității administrației publice locale, s-a subliniat faptul că este necesară luarea în considerare a aspectelor detaliate în considerentele Regulamentului (UE) 2016/679, astfel:

„(38) Copiii au nevoie de o protecţie specifică a datelor lor cu caracter personal, întrucât pot fi mai puţin conştienţi de riscurile, consecinţele, garanţiile în cauză şi drepturile lor în ceea ce priveşte prelucrarea datelor cu caracter personal. Această protecţie specifică ar trebui să se aplice în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator şi la colectarea datelor cu caracter personal privind copiii în momentul utilizării serviciilor oferite direct copiilor. Consimţământul titularului răspunderii părinteşti nu ar trebui să fie necesar în contextul serviciilor de prevenire sau consiliere oferite direct copiilor.

(75) Riscul pentru drepturile şi libertăţile persoanelor fizice, prezentând grade diferite de probabilitate de materializare şi de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: (...) sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii (...).”

Pe de altă parte, s-a apreciat ca fiind necesară și luarea în considerare a dispozițiilor Legii nr. 272/2004 privind protecţia şi promovarea drepturilor copilului, republicată.

Referitor la dispozițiile art. 8 din Regulamentul (UE) 2016/679, s-a menționat faptul că acestea sunt aplicabile în contextul funcționării „sistemului e-ticheting cu carduri” numai în măsura în care are loc oferirea de servicii ale societăţii informaţionale în mod direct unui copil.

În acest context, s-a arătat faptul că, potrivit art. 1 alin. (1) lit. b) din Directiva nr. 1535/2015 referitoare la procedura de furnizare de informaţii în domeniul reglementărilor tehnice şi al normelor privind serviciile societăţii informaţionale, „serviciu” înseamnă „orice serviciu al societăţii informaţionale, adică orice serviciu prestat în mod normal în schimbul unei remuneraţii, la distanţă, prin mijloace electronice şi la solicitarea individuală a beneficiarului serviciului.”

► ***Valabilitatea consimțământului on-line al părinților pentru prelucrarea datelor lor și ale copiilor***

Un operator a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la valabilitatea obținerii acordului părinților pentru prelucrarea datelor lor și ale copiilor în scopul înscrierii în tabere, modalitatea aleasă fiind completarea unui formular Google.

Referitor la modalitatea de prelucrare a datelor cu caracter personal, inclusiv sub aspectul colectării, stocării, divulgării prin transmitere, diseminarea sau punerea la dispoziţie 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.

De asemenea, art. 7 din Regulamentul sus-menționat prevede următoarele:

„(1) În cazul în care prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal.

(2) În cazul în care consimţământul persoanei vizate este dat în contextul unei declaraţii scrise care se referă şi la alte aspecte, cererea privind consimţământul trebuie să fie prezentată într-o formă care o diferenţiază în mod clar de celelalte aspecte, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Nicio parte a respectivei declaraţii care constituie o încălcare a prezentului Regulament nu este obligatorie.

(3) Persoana vizată are dreptul să îşi retragă în orice moment consimţământul. Retragerea consimţământului nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimţământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca acordarea acestuia.

(4) Atunci când se evaluează dacă consimţământul este dat în mod liber, se ţine seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiţionată sau nu de consimţământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.”

Totodată, considerentul 32 din Regulamentul (UE) nr. 2016/679 stabilește următoarele: „Consimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuțe atunci când persoana vizitează un site, alegerea

parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu ar trebui să constituie un consimțământ. Consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării. În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul."

În același timp, s-a precizat că în documentul intitulat "Orientări asupra Consimțământului în temeiul Regulamentului 2016/679" (WP 259), fostul Grup de Lucru Art. 29 (în prezent Comitetul european pentru protecția datelor) se menționează 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".

De asemenea, în același document se precizează faptul că: „Consimțământul nu va fi liber în cazurile în care există vreun element de constrângere, presiune sau incapacitate de exercitare liberă a voinței.", precum și faptul că „includerea (în RGPD) unor prevederi și considerente specifice asupra retragerii consimțământului confirmă faptul că acordarea consimțământului trebuie să constituie o decizie reversibilă și este menținut un grad de control de către persoana vizată."

În plus, s-a subliniat faptul că un aspect important pe care Regulamentul (UE) 2016/679 îl reglementează, iar operatorii trebuie să îl respecte, este reprezentat de informarea persoanelor vizate (indiferent de temeiul legal al prelucrării). În acest sens, art. 12 din Regulamentul (UE) 2016/679 prevede că operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informaţii menţionate la articolele 13 şi 14 şi orice comunicări în temeiul articolelor 15-22 şi 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special pentru orice informaţii adresate în mod specific unui copil.

În același timp, s-a menționat că operatorul trebuie să asigure măsurile tehnice și organizatorice în conformitate cu art. 32 și art. 25 din Regulamentul (UE) 2016/679.

► ***Anonimizarea datelor candidaților la concursuri***

Un operator, instituție de învățământ superior, a solicitat punctul de vedere al Autorității naționale de supraveghere cu privire la necesitatea inserării în acordul de prelucrare a datelor cu caracter personal a persoanelor care vor da concurs pentru ocuparea unui post, a unei clauze specifice prin care se optează cu privire la anonimizarea numelui și prenumelui până la finalizarea concursului.

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

Raportat la prevederile legale menționate mai sus, în măsura în care nu există o prevedere legală care să permită în mod expres publicarea numelor candidaților, s-a menționat că datele pot fi prelucrate (inclusiv publicate) de operatorii de date cu caracter personal pe baza existenței consimțământului persoanelor vizate.

Totodată, s-a atras atenția asupra faptului că operatorii trebuie să asigure măsurile tehnice și organizatorice în conformitate cu art. 32 și art. 25 din Regulamentul (UE) 2016/679.

► ***Montarea unor camere video în perimetrul apartamentului proprietate personală***

Mai multe persoane fizice au solicitat opinia Autorității naționale de supraveghere cu privire la condițiile de montare a unor camere video în perimetrul apartamentului proprietate personală.

Față de conținutul solicitării, s-au precizat următoarele:

Prelucrarea datelor cu caracter personal prin utilizarea unor sisteme de televiziune cu circuit închis cu posibilităţi de înregistrare şi stocare a imaginilor şi datelor se supune atât prevederilor Regulamentului (UE) 2016/679, cât şi ale Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor, modificată şi completată.

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

De asemenea, Autoritatea națională de supraveghere a menționat că în situația în care se are în vedere instalarea camerelor video pentru uzul personal, art. 2 alin. 2 lit. c) din Regulamentul (UE) 2016/679 prevede că acest act normativ european nu se aplică prelucrării datelor cu caracter personal efectuate de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice.

În plus, considerentul 18 din Regulament stabilește că „prezentul regulament nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice şi care, prin urmare, nu are legătură cu o activitate profesională sau comercială. Activităţile personale sau domestice ar putea include corespondenţa şi repertoriul de adrese sau activităţile din cadrul reţelelor sociale şi activităţile online desfăşurate în contextul respectivelor activităţi.”

Prin urmare, în situația în care sistemul de supraveghere video montat de o persoană fizică este orientat doar asupra propriului imobil ori bunului personal, pentru uzul exclusiv personal, sunt aplicabile prevederile art. 2 alin. 2 lit. c) din Regulament.

În sens contrar, în măsura în care persoana fizică a avut în vedere să panorameze și spațiul public se aplică Regulamentul (UE) 679/2016.

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

Autoritatea națională de supraveghere a precizat că în spaţiile monitorizate trebuie instalată o pictogramă adecvată, care să conţină o imagine reprezentativă, poziţionată la o distanţă rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere, astfel încât să poată fi văzută de orice persoană.

De asemenea, art. 13 din Regulamentul (UE) 679/2016 prevede că în cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obţinerii acestor date cu caracter personal, furnizează persoanei vizate informaţiile prevăzute de aceste dispoziții legale.

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

În plus, Autoritatea națională de supraveghere a recomandat ca perioada de stocare a datelor cu caracter personal (imaginea) prelucrate ca urmare a instalării sistemului de supraveghere video să nu depăşească 30 de zile.

► ***Legalitatea publicării declaraţiei de căsătorie pe internet de către autoritatea administrației publice locale***

O persoană fizică a solicitat opinia Autorității naționale de supraveghere cu privire la legalitatea publicării declaraţiei de căsătorie pe internet de către autoritatea administrației publice locale.

Față de acest aspect, instituția noastră a precizat faptul că, în ceea ce privește legalitatea prelucrării datelor, Regulamentul (UE) 2016/679 stabilește că prelucrarea datelor cu caracter personal se realizează la consimțământul persoanei vizate sau în alte

condiții legale în care nu se solicită consimțământul, prevăzute de art. 6, art. 9 și art. 10, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

În acest context, dispozițiile art. 238 din Codul civil stabilesc următoarele:

„(1) În aceeaşi zi cu primirea declaraţiei de căsătorie, ofiţerul de stare civilă dispune publicarea acesteia, prin afişarea în extras, într-un loc special amenajat la sediul primăriei şi pe pagina de internet a acesteia unde urmează să se încheie căsătoria şi, după caz, la sediul primăriei unde celălalt soţ îşi are domiciliul sau reşedinţa.

(2) Extrasul din declaraţia de căsătorie cuprinde, în mod obligatoriu: data afişării, datele de stare civilă ale viitorilor soţi şi, după caz, încuviinţarea părinţilor sau a tutorelui, precum şi înştiinţarea că orice persoană poate face opoziţie la căsătorie, în termen de 10 zile de la data afişării."

De asemenea, s-a menționat faptul că art. 5 din Regulamentul (UE) 679/2016 stabilește o serie de principii care se impun a fi respectate în cadrul prelucrării datelor. Printre acestea, se numără cele privind prelucrarea datelor în mod legal, echitabil şi transparent faţă de persoana vizată, prelucrarea datelor adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (principiul reducerii la minimum a datelor, respectiv al prelucrării datelor strict necesare îndeplinirii scopului), colectarea datelor în scopuri determinate, explicite şi legitime şi prelucrarea ulterioară într-un mod compatibil cu aceste scopuri, precum și prelucrarea de date exacte**.**

Prin urmare, s-a precizat că, raportat la dispozițiile legale mai sus menționate, datele personale pot fi prelucrate (dezvăluite) în condițiile din Regulamentul (UE) 679/2016, respectiv pe baza consimțământului sau a altor situații legale (cum este, în speță, îndeplinirea unei obligații legale), după caz, cu informarea prealabilă a persoanelor vizate.

► ***Legalitatea prelucrării datelor în contextul înregistrării și publicării pe internet a imaginilor cu numerele de înmatriculare ale autovehiculelor ai căror șoferi săvârșesc posibile contravenții sau infracțiuni în contextul circulației pe drumurile publice***

O persoană fizică a solicitat opinia Autorității naționale de supraveghere cu privire la legalitatea prelucrării datelor în contextul înregistrării și publicării pe internet a

imaginilor cu numerele de înmatriculare ale autovehiculelor ai căror șoferi săvârșesc posibile contravenții sau infracțiuni în contextul circulației pe drumurile publice.

S-a arătat că informațiile referitoare la numerele de înmatriculare ale autoturismelor reprezintă date cu caracter personal, deoarece conduc la identificarea în mod indirect a proprietarilor – persoane fizice – ale vehiculelor respective.

Prin urmare, persoana fizică sau juridică care prelucrează date de natura celor mai sus menționate are calitatea de operator de date cu caracter personal și obligația de a respecta prevederile legale din domeniul protecției datelor.

Autoritatea națională de supraveghere a precizat că la art. 6 din Regulamentul (UE) 679/2016 se stabilește că prelucrarea este legală numai dacă și în măsura în care persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice sau prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului.

Referitor la consimțământul persoanelor vizate, s-a menționat că acesta trebuie acordat în condițiile art. 7 din Regulamentul (UE) 679/2016, care prevede, printre altele, faptul că operatorul trebuie să fie în măsură să demonstreze că persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal.

În acest context, raportat la publicarea pe internet a unor date cu caracter personal, s-a precizat faptul că diseminarea în spațiul virtual a datelor persoanelor fizice în cauză și, implicit, punerea la dispoziția unui număr potențial foarte mare de persoane, fără niciun control asupra utilizării ulterioare a datelor în scopuri posibil incompatibile cu scopul inițial, poate reprezenta o ingerință gravă în drepturile la viaţă privată și protecția datelor cu caracter personal, astfel cum sunt garantate de art. 26 din Constituție, art. 8 din Convenţia Europeană a Drepturilor Omului, precum și art. 7 și 8 din Carta Drepturilor Fundamentale a UE.

În acest context, s-a menționat că Legea nr. 363/2018 reglementează 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.

Potrivit art. 1 alin. (2) din această lege, „Prelucrarea datelor cu caracter personal pentru realizarea activităţilor de menţinere şi asigurare a ordinii şi siguranţei publice se realizează numai dacă acestea sunt prevăzute de lege şi sunt necesare pentru prevenirea unui pericol cel puţin asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea infracţiunilor."

În considerarea dispozițiilor legale sus-menționate, s-a apreciat că prelucrarea de date preconizată (respectiv înregistrarea și publicarea pe internet a imaginilor cu numerele de înmatriculare ale autovehiculelor ai căror șoferi săvârșesc posibile contravenții sau infracțiuni în contextul circulației pe drumurile publice), nu respectă principiile prelucrării datelor, în special cel al legalității, iar monitorizarea respectării dispozițiilor legale în domeniul circulației pe drumurile publice este atribuția autorităților competente.

► ***Aplicarea normelor Regulamentului (UE) 679/2016 în contextul procedurii de termoscanare a persoanelor fizice***

În contextul punerii în aplicare a măsurilor pentru prevenirea infecției cu Sars-Cov2, mai multe persoane au adresat solicitări Autorității naționale de supraveghere cu privire la aplicarea normelor Regulamentului (UE) 679/2016 în contextul procedurii de termoscanare a persoanelor fizice la intrarea într-o anumită incintă.

În acest context s-a precizat că, în ceea ce privește informațiile ce pot fi considerate date cu caracter personal, potrivit art. 4 pct. 1 din Regulamentul (UE) 2016/679 „datele cu caracter personal" înseamnă „orice informaţii privind o persoană fizică identificată sau identificabilă („persoana vizată")".

Totodată, în ceea ce privește temperatura corpului, potrivit definiției „datelor privind sănătatea", acestea înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia.

Referitor la stocarea temperaturii corpului, conform art. 4 pct. 2 din Regulamentul (UE) 679/2016, prelucrarea înseamnă „orice operaţiune sau set de operaţiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea,

organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea".

De asemenea, potrivit art. 4 pct. 6 din Regulamentul (UE) 679/2016 „sistem de evidenţă a datelor" înseamnă „orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcţionale sau geografice".

Prin urmare, numai în măsura în care informațiile privind temperatura corporală a unei persoane fizice identificate sau identificabile se colectează, înregistrează, stochează, etc. într-un sistem de evidență, potrivit diferitelor mijloace de prelucrare, dispozițiile Regulamentului (UE) 2016/679 devin aplicabile.

În caz contrar, în ceea ce privește posibilele atingeri aduse altor drepturi și libertăți fundamentale decât cel garantat de art. 26 din Constituție, în contextul instituirii stării de alertă declarate potrivit legii, s-a apreciat că acestea se impun a fi aduse în atenția altor autorități competente, iar nu Autorității naționale de supraveghere.

În acest context, s-a precizat faptul că, potrivit art. 2 din Ordinul nr. 874/81 din 22 mai 2020 privind instituirea obligativităţii purtării măştii de protecţie, a triajului epidemiologic şi dezinfectarea obligatorie a mâinilor pentru prevenirea contaminării cu virusul SARS-CoV-2, „Pe durata stării de alertă se instituie obligativitatea instituţiilor şi autorităţilor publice, operatorilor economici şi profesioniştilor de a organiza activitatea astfel încât să se asigure la intrarea în sediu efectuarea triajului epidemiologic şi dezinfectarea obligatorie a mâinilor, în condiţiile şi cu respectarea Instrucţiunilor generale privind măsurile de igienă, prevăzute în anexă."

► ***Prelucrarea datelor în contextul marketingului direct***

O entitate privată a solicitat Autorității naționale de supraveghere un punct de vedere referitor la acordarea consimțământului pentru prelucrarea datelor în contextul marketingului direct.

Autoritatea națională de supraveghere a precizat cu privire la modalitatea de prelucrare a datelor cu caracter personal, inclusiv sub aspectul colectării, stocării, divulgării prin transmitere, diseminării sau punerii la dispoziţie în orice alt mod, potrivit Regulamentului (UE) 2016/679, că aceasta se realizează cu consimțământul persoanei

vizate sau în celelalte condiții prevăzute de art. 6, art. 9 și art. 10 din același act normativ, în funcție de natura datelor și categoriilor de date colectate și prelucrate.

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) menționează 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".

De asemenea, în același document se precizează: „Consimțământul nu va fi liber în cazurile în care există vreun element de constrângere, presiune sau incapacitate de exercitare liberă a voinței", precum și faptul că „includerea [în Regulamentul (UE) 2016/679] unor prevederi și considerente specifice asupra retragerii consimțământului confirmă faptul că, acordarea consimțământului trebuie să constituie o decizie reversibilă și este menținut un grad de control de către persoana vizată."

Totodată, în același document se 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. Regulamentul (UE) 2016/679 nu exclude toate stimulentele, dar îi revine operatorului sarcina să demonstreze că consimțământul a fost exprimat în continuare în mod liber în toate circumstanțele."

Ca atare, obținerea consimțământului persoanei vizate, în măsura în care prelucrarea are loc pe baza acestuia, trebuie să îndeplinească condițiile din Regulamentul (UE) 2016/679 menționate mai sus.

Un aspect important pe care Regulamentul (UE) 2016/679 îl reglementează, iar operatorii trebuie să îl respecte, este reprezentat de informarea persoanelor vizate (indiferent de temeiul prelucrării, la consimțământ sau pe baza celorlalte condiții de prelucrare).

În sensul celor de mai sus este considerentul (70) din Regulamentul (UE) 2016/679 „În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată ar trebui să aibă dreptul de a se opune unei astfel de prelucrări, inclusiv creării de profiluri în măsura în care aceasta are legătură cu marketingul direct, indiferent dacă prelucrarea în cauză este cea inițială sau una ulterioară, în orice moment şi în mod gratuit. Acest drept ar trebui adus în mod explicit în atenţia persoanei vizate şi prezentat în mod clar şi separat de orice alte informaţii."

În același timp, operatorul trebuie să respecte principiile de prelucrare stabilite în art. 5 din Regulamentul (UE) 2016/679 și să asigure, totodată, măsurile tehnice și organizatorice în conformitate cu art. 32 și art. 25 din același Regulament.

Totodată, 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, de a decide cu privire la legitimitatea prelucrării și, în același timp, de a lua toate măsurile necesare pentru respectarea drepturilor persoanelor vizate, precum și pentru asigurarea securității și confidențialității datelor, raportat la prevederile legale mai sus menționate.

► ***Prelucrarea datelor angajaților în contextul derulării activității de telemuncă***

O entitate privată a solicitat un punct de vedere cu privire la legalitatea supravegherii angajaților în contextul în care aceștia derulează activități de telemuncă.

În ceea ce privește supravegherea angajaților, Autoritatea națională de supraveghere a precizat că dispozițiile art. 5 din Legea nr. 190/2018 stabilesc următoarele:

„În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea

datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

a) interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;

b) angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;

c) angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;

d) alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa; şi

e) durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate."

Prin urmare, supravegherea angajaților la locul de muncă se poate institui numai în condițiile mai sus stabilite de lege, aspecte care trebuie să se regăsească la angajator într-o documentație argumentată temeinic, din care să rezulte prevalența interesului legitim asupra intereselor sau drepturilor şi libertăţilor angajaților.

Totodată, raportat la prevederile legale sus-menționate, s-a precizat că informarea persoanelor vizate trebuie realizată, indiferent de legitimitatea prelucrării datelor, iar sub aspectul conținutului informării, acesta trebuie să respecte dispozițiile art. 13 din Regulamentul (UE) 2016/679.

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

Așadar, prelucrarea datelor cu caracter personal ale angajaților prin utilizarea unor mijloace de supraveghere a acestora, este supusă obligației de respectare a condițiilor de legalitate (inclusiv art. 6 din Regulamentul (UE) 2016/679), precum și a măsurilor de confidențialitate și securitate a datelor cu caracter personal pentru a se asigura protecția acestora, precum și respectarea drepturilor persoanelor vizate, în conformitate cu Regulamentul (UE) 679/2016.

Totodată, Autoritatea națională de supraveghere a menționat că activității de telemuncă îi sunt aplicabile și dispozițiile Legii nr. 81/2018 privind reglementarea activității de telemuncă, care prevede, printre altele, că „Angajatorul este în drept să verifice activitatea telesalariatului, în condițiile stabilite prin contractul individual de muncă, regulamentul intern și/sau contractul colectiv de muncă aplicabil, în condițiile legii."

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

În anul 2020 au fost transmise puncte de vedere ale Autorității naționale de supraveghere către Ministerul Afacerilor Externe, în **15 cauze** pendinte în fața Curții de Justiție a Uniunii Europene, referitoare la interpretarea anumitor articole din acte normative comunitare (Directiva 95/46/CE, Directiva 2002/58/CE, respectiv din Regulamentul (UE) 2016/679) astfel:

► **C-102/20 – StWL Städtische Werke Lauf a.d. Pegnitz GmbH** cererea fiind adresată Curţii de Justiţie a Uniunii Europene de o instanţă de trimitere din Germania (Bundesgerichtshof), referitoare la interpretarea dată **articolului 2 a doua teză litera (h) din Directiva 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice)**, respectiv cu privire la interpretarea noțiunii de poștă electronică, inclusiv prin raportare la articolul 13 alineatul (1) din Directiva 2002/58/CE în cazul folosirii sistemelor de apelare şi comunicare automate, fără intervenţie umană (maşini de apelare automată), a faxurilor sau a poştei electronice în scopuri de marketing direct.

► **C-793/19 – SpaceNet și alții**, cererea fiind adresată Curţii de Justiţie a Uniunii Europene de o instanţă de trimitere din Germania (Bundesverwaltungsgericht - Curtea Administrativă Federală, Germania), referitoare la **articolul 15 din Directiva 2002/58/CE**, citit în lumina articolelor 7, 8 și 11, precum și a articolului 52 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene, pe de o parte, și a articolului 6

din Carta drepturilor fundamentale a Uniunii Europene, precum și a articolului 4 din Tratatul privind Uniunea Europeană, respectiv dacă trebuie interpretat în sensul că se opune unei reglementări naționale care impune prestatorilor de servicii publice de comunicații electronice să păstreze datele de transfer și de localizare ale utilizatorilor finali ai acestor servicii în anumite condiții.

► **C-817/19 – ASBL „Ligue des droits humains”** cererea fiind adresată Curţii de Justiţie a Uniunii Europene de o instanţă de trimitere din Belgia (Curtea Constituțională), referitoare la interpretarea anumitor prevederi din **Legea/2016 privind prelucrarea datelor pasagerilor (Moniteur belge din 25 ianuarie 2017 - „Legea PNR”) care transpune în principal Directiva (UE) 2016/681** a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave („Directiva PNR”) și **Directiva 2004/82/CE** a Consiliului din 29 aprilie 2004 privind obligația operatorilor de transport de a comunica datele privind pasagerii („Directiva API”).

► Cauzele conexate **C-148/20 – C-150/20 – Deutsche Lufthansa** cererea fiind adresată Curţii de Justiţie a Uniunii Europene de o instanţă de trimitere din Germania (Amtsgericht Köln), referitoare la interpretarea anumitor prevederi din **Legea privind prelucrarea datelor pasagerilor aerieni (Fluggastdatengesetz – „FlugDaG” din 10 iunie 2017) care transpune Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave („Directiva PNR”)**.

► Cauzele reunite **C-339/20 și C-397/20 – ”VD și alții”** cererile fiind adresate Curţii de Justiţie a Uniunii Europene de o instanță de trimitere din Franța (Cour de Cassation, Chambre Criminelle), referitoare la interpretarea anumitor prevederi privind păstrarea datelor de conectare la care se face referire în **Directiva 2003/6/CE a Parlamentului European și a Consiliului din 28 ianuarie 2003 privind utilizările**

abuzive ale informațiilor confidențiale și manipulările pieței (abuzul de piață), precum și din **Regulamentul (UE) 596/2014 al Parlamentului European și al Consiliului din 16 aprilie 2014 privind abuzul de piață**, care a înlocuit directiva menționată anterior, începând de la data de 3 iulie 2016.

► **Cauza C-184/20** în cadrul căreia cererea a fost adresată de o instanță din Lituania, cu privire la interpretarea **art. 6 alin. (1) lit. e) coroborat cu art. 6 alin. (3), art. 9 alin. (1) coroborat cu art. 9 alin. (2) lit. g) din Regulamentul (UE) 2016/679, din perspectiva art. 7 și 8 din Carta UE.**

► **Cauza C-460/20** în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea **art. 17 alin. (3) lit. a) din Regulamentul (UE) 2016/679, din perspectiva art. 7, 8, 11 și 16 din Carta UE.**

► **Cauza C-534/20** în cadrul căreia cererea a fost adresată de o instanță din Germania, referitoare la interpretarea **art. 38 alin. (3) teza a II-a din Regulamentul (UE) 2016/679.**

► **Cauza E-11/19** în cadrul căreia cererea a fost adresată de o instanță din Liechtenstein, referitoare la interpretarea unor dispoziții din **Regulamentul (UE) 2016/679, în special articolul 77 din acesta.**

► **Cauza C-245/20 – Autoriteit Persoonsgegevens** (Olanda) (instanţă de trimitere din Olanda – Țările de Jos) în care s-au adresat întrebări preliminare, în contextul interpretării **articolului 55 alineatul (3) din Regulamentul (UE) 2016/679.**

► **Cauza C-175/20 – Valsts ienemumu dienests** (instanţă de trimitere din Letonia) în care s-au adresat întrebări preliminare legate de interpretarea cerințelor prevăzute de **Regulamentul (UE) 2016/679, în special articolul 5 alineatul (1) din acesta**.

► **Cauza C-140/20 Commissioner of the Garda Síochána and Others** (instanţă de trimitere din Irlanda - Supreme Court) în care s-au adresat întrebări preliminare, în contextul compatibilității legislației naționale cu **articolul 15 din Directiva 2002/58/CE în privința păstrării și accesului la date cu caracter personal, inclusiv în situația în care prelucrarea este supusă unor restricții stricte în materie de păstrare și de acces.**

► **Cauza E-10/19 – Bergbahn Aktiengesellschaft Kitzbühel v Meleda Anstalt**, (instanţă de trimitere din Lichstenstein - Fürstliches Obergericht) în care s-au adresat întrebări preliminare legate de interpretarea cerințelor prevăzute de **Directiva 2015/849 EU, în special articolul 30 (1) din aceasta.**

► **Cauza E-12/19** în cadrul căreia cererea a fost adresată de o instanță din Liechtenstein, referitoare la interpretarea dispozițiilor **art. 77 din Regulamentul (UE) 2016/679.**

► **Cauza C-319/20** în cadrul căreia cererea a fost adresată de o instanţă de trimitere din Bundesgerichtshof - Germania, referitoare la interpretarea **art. 80 alin. (1) și (2) și art. 84 alin. (1) din Regulamentul (UE) 2016/679.**

▪Puncte de vedere exprimate în contextul analizării codurilor de conduită

O organizaţie profesională în domeniul insolvenței din România a transmis un cod de conduită pentru eventuale recomandări privind corectarea sau completarea prevederilor în acord cu prevederile Regulamentului (UE) 2016/679.

Faţă de conținutul acestuia, s-a recomandat reanalizarea proiectului transmis astfel încât să prevadă măsuri și soluții particularizate activității membrilor organizației referitoare la respectarea Regulamentului (UE) 2016/679 în sectorul de activitate vizat.

Cât privește drepturile persoanelor vizate, s-a recomandat prezentarea clară a procedurii de exercitare a tuturor drepturilor, prin care să se prevadă modalitățile concrete de formulare și soluționare a cererilor adresate de persoanele vizate, inclusiv a termenelor de răspuns, în concordanță cu specificitatea fiecărui drept în parte.

Referitor la informarea persoanei vizate, s-a subliniat că aceasta trebuie să respecte dispozițiile art. 12, 13 și 14 din Regulamentul (UE) 2016/679, în funcție de modalitatea de colectare a datelor, direct sau indirect, cu precizarea în mod clar a aspectelor vizate de aceste dispoziții, pentru respectarea principiului transparenței.

Totodată, s-a precizat că, întrucât acest cod urmează să fie „implementat în mod unitar la nivelul tuturor structurilor coordonate", acesta trebuie redactat într-o manieră accesibilă tuturor operatorilor cărora li se adresează, pentru înțelegerea și aplicarea cu ușurință de către aceștia.

■ 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 secţiei de contencios administrativ a tribunalului competent, după parcurgerea procedurii prealabile prevăzute de Legea contenciosului administrativ nr. 554/2004, cu modificările şi completările ulterioare.

Astfel, pe parcursul anului 2020 au fost depuse la Autoritatea națională de supraveghere un număr de **18 plângeri prealabile**.

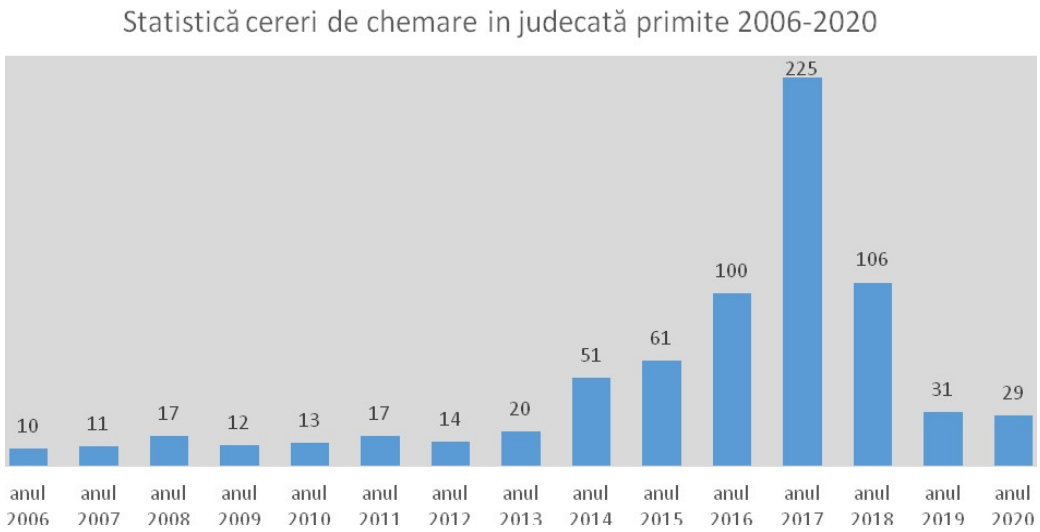
Dintre plângerile prealabile formulate în condițiile legii, urmare a reanalizării susținerilor și dovezilor transmise de către petenți, au fost admise 8, raportat la aspectele semnalate de către persoanele vizate în cauză.

Secțiunea a 4 – a
Activitatea de reprezentare în fața instanțelor de judecată

În anul 2020, Autoritatea națională de supraveghere a gestionat un număr de **127 dosare** aflate pe rolul instanțelor de judecată în diferite stadii procesuale.

Dintre acestea, pe parcursul anului 2020 au fost înregistrate pe rolul instanțelor de judecată un număr de **29 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 12 din cele 29 de cereri de chemare în judecată au avut ca obiect contestarea proceselor – verbale de constatare/sancționare încheiate de Autoritatea națională de supraveghere.



În anul 2020 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. 32 alin. (1) și (2) din Regulamentul (UE) 2016/679

Un operator din domeniul vânzărilor de automobile a notificat Autorității naționale de supraveghere o încălcare a securității datelor cu caracter personal, semnalând o dezvăluire a unor date cu caracter personal pe o pagină de Facebook a grupului de societăți din care face parte operatorul.

Astfel, pe pagina de socializare respectivă a fost publicat un document cu o captură din codul sursă al paginii de Internet care aparține operatorului și pe care acesta a desfășurat, în anul 2017, un concurs on-line de atragere a clienților participanți.

În codul sursă era inclusă și parola de acces la formularele completate de participanții la concurs. Extragerea și utilizarea parolei din codul sursă a condus la vizualizarea datelor cu caracter personal ale unui număr de peste patru sute de clienți ai operatorului, respectiv: nume și prenume, localitate, telefon, e-mail, autoturism deținut și serie de șasiu.

Urmare a investigației efectuate, s-a constatat faptul că operatorul a încălcat art. 32 alin. (1) și (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 pentru drepturile și libertățile persoanelor fizice, ceea ce a condus la divulgarea și accesul neautorizat la datele cu caracter personal ale unui număr de peste patru sute de clienți ai săi, deși potrivit art. 5 lit. f) din Regulamentul (UE) 2016/679, operatorul are obligația de a respecta principiul ,,integritate și confidențialitate".

Pentru fapta constatată s-a aplicat amendă în cuantum de 72.642,00 lei (echivalentul a 15.000 euro).

De asemenea, s-a dispus ca măsură corectivă „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, astfel încât să fie evitate incidente similare de dezvăluire neautorizată a datelor cu caracter personal prelucrate", întrucât, deși operatorul implementase o serie de măsuri la momentul desfășurării campaniei publicitare, acestea s-au dovedit a nu fi adecvate pentru a se asigura un nivel de securitate corespunzător riscurilor, respectiv pentru a se evita producerea incidentului de securitate.

Operatorul a contestat în instanță procesul-verbal de sancționare, dar plângerea contravențională a fost respinsă, tribunalul competent confirmând ca legale și temeinice măsurile luate de Autoritatea națională de supraveghere.

Astfel, instanța de judecată a statuat în mod corect faptul că *"în speță deși reclamanta susține că dezvăluirea datelor personale (...) nu a avut loc și că autoritatea a apreciat în mod greșit că divulgarea neautorizată a datelor personale ale celor participanți la concurs, respectiv nume, prenume, adresa, telefon, serie de șasiu, nu au fost divulgate niciunui terț autorizat sau neautorizat și nu au apărut în spațiul public, aceasta nu a dovedit prin probe solide o altă situație de fapt față de cea reținută și care*

din punct de vedere factual cade sub incidența dispozițiilor art. 32 alin. (1) și art. 32 alin. (2) din RGPD, ce au atras aplicarea sancțiunii pentru că nu au fost implementate măsuri tehnice și organizatorice adecvate (...)".

De asemenea, sub aspectul faptei săvârșite, instanța a constatat faptul că *"nu pot fi reținute argumentele referitoare la inexistența unei încălcări, de vreme ce aceasta [reclamanta] a recunoscut că a avut loc un incident de securitate pe care l-a notificat Autorității, sistemele sale au fost vulnerabile și posibil de accesat, a sesizat acest lucru și către Cert-RO, a apelat la un consultant IT și a luat ulterior incidentului o serie de măsuri tehnice și organizatorice, toate aceste aspecte contrazicând inexistența unei încălcări.*

În același sens, instanța opinează că obligația reclamantei era cu atât mai necesară cu cât aceasta a arătat că face parte din rețeaua unei corporații internaționale și a implementat "toate Regulile Corporative" ale grupului (...) al cărui dealer autorizat este.

Or, față de cele mai sus exprimate, instanța opinează că procesul verbal este temeinic și legal întocmit, neexistând vreun dubiu care să conducă la anularea sa."

Totodată, referitor la cererea formulată de către reclamantă în privința înlocuirii amenzii cu avertisment, instanța opinează că *"față de gravitatea faptei în aplicarea măsurii a fost respectat principiului proporționalității sancțiunii, cu atât mai mult cu cât din probele administrate a rezultat în mod vădit că reclamanta nu a depus toate diligențele pentru a lua și respecta măsurile tehnice și organizatorice adecvate pentru a asigura un nivel de securitate corespunzător riscurilor (...).*

De altfel, atunci când vine vorba despre natura sau gravitatea faptei legiuitorul a înțeles să îl individualizeze prin cuantumul amenzii, iar față de acest cuantum alte deziderate afară de lipsa de diligență a reclamantei sunt deja redundante."

Hotărârea instanței de fond favorabilă Autorității naționale de supraveghere a rămas definitivă.

2. Hotărâre definitivă pronunțată într-un litigiu privind nerespectarea dreptului de intervenție asupra datelor și a dreptului de opoziție prevăzut de art. 14 și 15 din Legea nr. 677/2001

Potrivit unei investigații efectuate de către Autoritatea națională de supraveghere, ca urmare a unei plângeri a unui petent prin care acesta sesiza încălcări ale prelucrării datelor de către un operator din domeniul financiar-bancar, prin scanarea, fără temei

legal a cărții sale de identitate și înregistrarea imaginii sale prin sistemul de supraveghere video, fără informarea prealabilă conform dispozițiilor art. 11 din Decizia 52/2012, dar și lipsa unui răspuns din partea operatorului cu privire la solicitările sale, s-a constatat încălcarea legislației în vigoare, fiind dispuse *sancțiuni cu avertisment și amendă*.

Astfel, operatorul de date a fost sancționat întrucât, pe lângă faptul că nu a făcut dovada că i-a comunicat un răspuns complet petentului, la cererea acestuia, a reţinut date conţinute în actul de identitate al acestuia, prin reţinerea copiei actului de identitate, fără consimţământul expres al petentului, în lipsa unui temei legal sau al unui aviz al Autorității naționale de supraveghere. Totodată operatorul nu a făcut dovada că a furnizat persoanelor vizate toate informațiile cu privire la existenţa sistemului de supraveghere.

Operatorul a contestat în instanță procesul-verbal de constatare/sancţionare.

Analizând probatoriul administrat în cauză, Tribunalul București a constatat că Procesul-verbal de constatare/sancţionare emis de Autoritatea națională de supraveghere este legal întocmit, fiind „respectate cerințele art 17 din OG nr. 2/2001 în raport de tipologia fiecărei contravenții în parte".

Cu privire la legalitatea procesului-verbal de contravenție, instanța a apreciat că acesta este temeinic, pronunțându-se pe fiecare contravenție în parte. Astfel, instanța a reținut că *„operatorul nu a făcut dovada, până la întocmirea procesului-verbal, că i-a comunicat un răspuns complet petentului, la cererea acestuia."*

Pe de altă parte, cu privire la prelucrarea copiei actului de identitate al petentului, instanța a reținut că *"în contextul în care Banca nu a demonstrat că operațiunea de plată efectuată de petiționar ar fi îndeplinit caracteristicile unei fapte ce intră sub incidența Legii nr. 656/2002, reținerea unei copii a cărții de identitate nu pare a fi justificată și, prin aceasta, nu apare a fi protejată de reglementarea invocată de Bancă.*

(...) nu s-ar putea susține în mod legitim că este acoperită de norma legală (care, de altfel, în cazul de față s-a dovedit a corespunde așteptărilor și a fi rezonabilă și rațională - art. 4 din Regulamentul nr. 9/2008) o practică nediferențiată de a fotocopia și de a reține o fotocopie a cărții de identitate în cazul oricărui serviciu prestat de institutia bancară."

În același timp, cu privire la existența unei informări la sediul operatorului referitoare la existenţa sistemului de supraveghere video, instanța a reținut că *"Banca*

este cea care ar fi putut și ar fi trebuit, în fața acuzației investigate (...) să probeze că la data de (...) își îndeplinise obligațiile impuse de art. 12 din Legea nr. 677/2001".

Cu privire la individualizarea sancțiunilor prin Procesul-verbal de constatare/sancţionare contestat, *Tribunalul a constatat că „sancțiunile aplicate sunt bine individualizate".*

Hotărârea instanței de fond, favorabilă Autorității naționale de supraveghere, a rămas definitivă prin respingerea apelului formulat de operator.

3. Hotărâre pronunțată într-un litigiu privind prelucrarea nelegală de date biometrice

Autoritatea națională de supraveghere a efectuat o investigație din oficiu la un operator din domeniul farmaceutic, având ca obiect verificarea modului de respectare a prevederilor Legii nr. 677/2001 şi ale Legii nr. 506/2004.

În urma investigației efectuate, Autoritatea națională de supraveghere a constatat săvârșirea de fapte contravenționale de către acest operator.

Astfel, pe de o parte operatorul, deși a început cu mult anterior să utilizeze sistemul de pontare electronică a angajaților pe baza datelor biometrice - amprente, nu a notificat la Autoritatea națională de supraveghere anterior începerii prelucrării, conform obligațiilor prevăzute de art. 22 alin. (1) din Legea nr. 677/2001.

Pe de altă parte, operatorul a prelucrat date biometrice considerate a fi excesive față de scopul prelucrării, respectiv, pontarea timpului de lucru al angajaților, putând fi utilizate și alte mijloace pentru atingerea acestui scop, mai puțin intruzive, încălcându-se astfel art. 4 alin. 1 lit. c) din Legea nr. 677/2001.

Pentru faptele constatate operatorul a fost sancţionat contravenţional.

Totodată, operatorului i s-a solicitat să înceteze prelucrarea datelor biometrice (amprente) ale angajaților, colectate în scopul efectuării pontajului și să șteargă din sistemul propriu de evidență amprentele colectate.

Procesul-verbal de constatare/sancţionare contravenţională a fost contestat la instanţa competentă.

Curtea de Apel a arătat că *„esențial este aspectul că nu era necesară prelevarea amprentelor angajaților în scop de pontaj, câtă vreme pontajul se face după seria*

cardului, prelucrarea datelor biometrice fiind astfel excesivă prin raportare la scopul declarat (pontaj).

Mai mult, la nivelul intimatei - reclamante s-a constatat utilizarea, simultan, a unor mijloace diferite de atingere a aceluiași scop (pontajul), respectiv pe bază de amprentă ori pe bază de cod PIN asociat cardului angajaților acesteia, prin urmare puteau fi folosite și mijloace mai puțin intruzive pentru atingerea scopului iar prelucrarea datelor biometrice nu poate fi considerată drept o măsură legitimă.(...)

Indiscutabil, sistemul de pontare utilizat de intimată atrage beneficii economice cu referire la faptul că numărul orelor suplimentare ar fi scăzut, în pofida creșterii numărului angajaților din farmacii însă nu aceasta este analiza care trebuie efectuată din perspectiva prevederilor art. 4 alin. (1) lit. c) din Legea nr. 677/2001, măsura implementată nefiind una proporțională sens în care se impune a fi validată teza autorității potrivit căreia societatea colectează excesiv date biometrice ale persoanelor fizice (angajați), raportat la scopul prelucrării (pontaj).(...)

Măsura este una intruzivă și nu trece testul proporționalității, nefiind strict necesară pentru scopul declarat în vederea căruia a fost adoptată."

Cu privire la vinovăție Curtea de Apel a apreciat că *„se impun a fi înlăturate cele statuate de instanța de fond. Societatea este un profesionist, fiind de netăgăduit că nu se poate reține lipsa intenției în sensul că aceasta nu a prevăzut, acceptat or ar fi trebuit să prevadă o ingerință în dreptul la viața privată al salariaților neproporțională cu scopul urmărit ori neprevăzută de lege, sau că nu ar fi prevăzut, nu ar fi acceptat ori nu ar fi trebuit să prevadă că prelucrarea de date biometrice era excesivă în raport cu scopul urmărit."*

Pe cale de consecință, Curtea de Apel a apreciat că procesul - verbal de constatare și sancționare a contravenției *„apare ca fiind legal emis, sancțiunea fiind corect individualizată având în vedere prevederile art. 21 din OG 2/2001 raportat la art. 32 si 35 din Legea nr. 677/2001"*. De asemenea, aceeași instanță a apreciat că *„apare ca fiind legală recomandarea de încetare a prelucrării datelor biometrice și de ștergere din sistemul operatorului a amprentelor colectate"*.

Hotărârea judecătorească favorabilă Autorității naționale de supraveghere a rămas definitivă.

Secțiunea a 5 -a

Informare publică

Autoritatea naţională de supraveghere a continuat, în anul 2020, **activităţile 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 Protecţiei Datelor – 28 Ianuarie 2020**

Pentru sărbătorirea Zilei Europene a Protecţiei Datelor în anul 2020, Autoritatea naţională de supraveghere a organizat Conferința cu tema **„Aspecte practice de aplicare a Regulamentului General privind Protecția Datelor și a reglementărilor naționale incidente”,** la Palatul Parlamentului, pe data de **31 Ianuarie 2020.**

Acest eveniment a oferit prilejul unor dezbateri cu privire la aplicarea noilor exigențe ale Regulamentului (UE) 2016/679, ale Legii nr. 129/2018 și ale Legii nr. 190/2018, raportat și la competențele Autorității naționale de supraveghere.

De asemenea, 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.

Totodată, pe postul național de televiziune TVR și în mijloacele de transport STB, s-a difuzat în anul 2020 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, **iar la sediul Autorității a fost organizată ”Ziua Porților Deschise”.**

♦ **Eveniment aniversar - doi ani de la aplicarea Regulamentului (UE) 2016/679 – 25 Mai 2020**

Cu prilejul sărbătoririi a doi ani de la aplicarea Regulamentului (UE) 679/2016, Autoritatea naţională de supraveghere a organizat, în luna mai 2020, un **concurs on-line de desene pentru copii** cu vârsta de până la 14 ani, cu tema: „Ce înseamnă datele personale/protecția datelor personale". Acest eveniment a urmărit încurajarea implicării copiilor în conștientizarea semnificațiilor datelor personale într-o manieră expresivă și originală.

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 2020 la **reuniuni** cu incidență în domeniul protecției datelor, organizate de diverse instituții publice sau de entități private, **inclusiv 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 online** , cum ar fi:

- la Conferința națională GDPR „Data Protection – Soluții și responsabilități", organizată on-line de Grupul editorial Universul Juridic și Revista Română pentru Protecţia și Securitatea Datelor cu Caracter Personal (RRPSDCP), prin susținerea unei prelegeri privind rolul si competențele Autorității naționale de supraveghere;
- la Agenția Națională a Funcționarilor Publici, la seminariile ocazionate în cadrul derulării proiectului "Instruire în domeniul prelucrării datelor cu caracter personal

pentru structurile din cadrul sistemului de coordonare, gestionare și control al FESI în România";

- la Agenția Națională a Funcționarilor Publici, la reuniunea privind protecția datelor în cadrul fondurilor europene din 02.10.2020;
- la Ministerul Lucrărilor Publice, Dezvoltării și Administrației, la atelierul de lucru cu tema "Dezbaterea aspectelor evidențiate în cadrul procesului de analiză a legislației aplicabile, a situațiilor și a dificultăților întâlnite în practică de către autoritățile și instituțiile publice în ceea ce privește principalele categorii de acte și contracte administrative" organizat în cadrul proiectului „Instrumente de sistematizare a legislației, de monitorizare și de evaluare în administrația publică";
- la workshop-ul "Mobilitatea, o provocare pentru aplicarea GDPR", prin susținerea unei prelegeri privind aspecte practice și teoretice referitoare la problematica securizării informației purtătoare de date cu caracter personal la nivelul dispozitivelor mobile;
- la webinarul european "The DPO in times of Covid 19", organizat de Asociația Specialiștilor în Confidențialitatea și Protecția Datelor (ASCPD) alături de Confederația Organizațiilor Europene pentru Protecția Datelor (CEDPO);
- la reuniunea Grupului de lucru Dapix, alături de reprezentanți ai Ministerului Afacerilor Interne;
- la o videoconferință cu membrii Camerei de Comerț Româno-Americană (AmCham România), ocazie cu care s-au discutat aspecte privind modalitatea de aplicare a dispozițiilor Regulamentului (UE) 2016/679 referitoare la transferul datelor cu caracter personal către țări din afara Uniunii Europene, ca urmare a Deciziei Curții de Justiție a Uniunii Europene în Cauza Schrems II (C-311/18).

Pe de altă parte, subliniem că **s-a acordat consiliere telefonică** multor 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 pandemiei declanșate din luna martie 2020.

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: Direcția de Evidență a Persoanelor și Administrarea Bazelor de Date, Oficiul Român de Prevenire și Combatere a Spălării Banilor, Banca Națională a României, Ministerul Educației și Cercetării, Ministerul Dezvoltării Regionale și Administrației Publice, Ministerul Afacerilor Interne, Autoritatea pentru Digitalizarea României.

Autoritatea națională de supraveghere a participat și la **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, inclusiv transferul datelor cu caracter personal către țări din afara Uniunii Europene, ca urmare a Deciziei Curții de Justiție a Uniunii Europene în Cauza Schrems II (C-311/18).

Astfel, au avut loc întâlniri cu Camera de Comerț Româno-Americană (AmCham), Asociația Română a Băncilor (ARB), Biroul Român de Audit Transmedia (BRAT), Consiliul Investitorilor Străini (FIC), Asociația pentru Tehnologie și Internet (ApTI), Organizația Privacy International**.**

De asemenea, în vederea creşterii gradului de conştientizare cu privire la obligaţiile ce le revin operatorilor, potrivit prevederilor Regulamentului (UE) 2016/679, Autoritatea naţională de supraveghere a propus Asociației Municipiilor din România și Asociației Comunelor din România să-i acorde sprijinul în scopul anunțării tuturor membrilor asociațiilor cu privire la obligativitatea numirii și anunțării la Autoritatea națională de supraveghere a responsabilului desemnat la nivelul fiecărei autorități publice locale (comuna, oraș, municipiu), potrivit art. 37 din Regulamentul (UE) 2016/679.

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

Prin intermediul site-ului Autorității naționale de supraveghere s-a realizat o informare promptă şi eficientă a persoanelor fizice, dar și a operatorilor, atât prin prisma celor **60 de comunicate de presă** postate la secțiunea „Știri", cât și a informațiilor de la secțiunea specială dedicată Regulamentului (UE) 2016/679. În acest context, instituția noastră a continuat să publice amenzile dispuse în anul 2020, 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.

Raportat la problematica specifică anului 2020, Autoritatea națională de supraveghere a dat publicității un comunicat de presă intitulat *„Prelucrarea datelor cu caracter personal în contextul alegerilor pentru autorităţile administraţiei publice locale"*, având în vedere obligația entităților implicate în acest proces să acorde o atenție sporită respectării legislației privind protecția datelor cu caracter personal, pentru a se asigura că datele personale sunt utilizate în mod responsabil și că drepturile persoanelor vizate sunt respectate. Totodată, Autoritatea națională de supraveghere a dat publicității un comunicat de presă intitulat *„Prelucrarea datelor de către asociațiile de proprietari"*, ce explică pe larg modalitatea de prelucrare a datelor de către asociațiile de proprietari și obligațiile ce le revin.

Pe de altă parte, operatorii din sectorul public și privat au continuat să declare, utilizand formularul online pus la dispoziție, **responsabilii cu protecția datelor**, în anul 2020 înregistrându-se la Autoritatea naţională de supraveghere un număr de **2081** responsabili.

Un alt aspect relevant din activitatea desfășurată constă în preocuparea manifestată pentru **creșterea gradului de accesibilitate digitală** in interacțiunea persoanelor fizice și operatorilor cu instituția noastră. Astfel, ca și anii precedenți, o atenție deosebită a fost acordată încurajării utilizării **formularelor on-line** puse la dispoziție de instituția noastră începând cu anul 2018, prin care operatorii pot declara electronic responsabilii cu protecția datelor sau pot notifica incicentele de securitate, precum și formularul de plângere on-line prin care persoanele fizice pot semnala încălcarea regulilor de protecție a datelor personale.

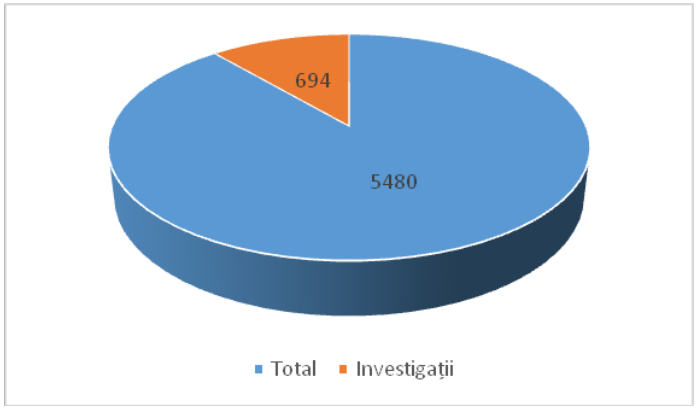
CAPITOLUL III

ACTIVITATEA DE MONITORIZARE ȘI CONTROL

Secțiunea 1. Prezentare generală

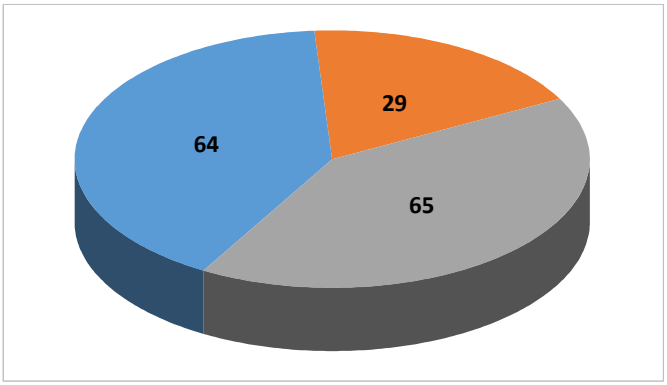
Și în anul 2020, o componentă importantă a activității Autorității naționale de supraveghere a reprezentat-o monitorizarea și controlul legalității prelucrărilor de date personale, prin intermediul investigațiilor efectuate fie din oficiu, fie în scopul soluționării plângerilor și sesizărilor primite.

În anul 2020, Autoritatea națională de supraveghere a primit un număr total de **5480** de plângeri, sesizări și notificări privind incidente de securitate, pe baza cărora au fost deschise **694 investigații**.



Ca urmare a investigațiilor, au fost aplicate **29 de amenzi** în cuantum total **de 892.115,95 lei.**

De asemenea, au mai fost aplicate **64 de avertismente** și au fost dispuse **65 de măsuri corective.**



În ceea ce privește soluționarea plângerilor și a sesizărilor, pe fondul menținerii numărului semnificativ al acestora (5082), în anul 2020 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;
- raportarea de date personale la Biroul de Credit.

Referitor la incidentele de securitate transmise 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.

Prin intermediul sesizărilor transmise au fost semnalate, în principal, aspecte referitoare la: lipsa măsurilor de securitate, inclusiv la nivelul website-urilor, publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele sociale.

Măsurile corective dispuse în urma plângerilor și a 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;
- ✓ 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;
- ✓ 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.

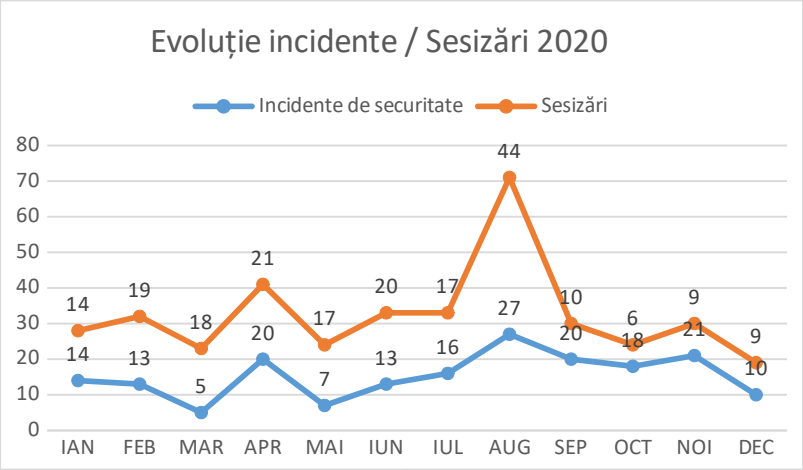
Secțiunea a 2 – a: Investigații din oficiu

1. Prezentare generală

În anul 2020, investigațiile din oficiu au urmărit cu prioritate obiective legate de respectarea dispozițiilor legale aplicabile în cadrul prelucrării datelor cu caracter personal, atât în sistemul public, cât și în cel privat.

Investigațiile din oficiu efectuate au avut ca obiect verificarea modului de respectare a prevederilor Regulamentului (UE) 2016/679, Legii nr. 190/2018, precum și a dispozițiilor Legii nr. 506/2004.

Astfel, în anul 2020, în ceea ce privește **incidentele de securitate**, operatorii de date cu caracter personal au transmis, atât în temeiul Regulamentului (UE) 2016/679, cât și al Legii nr. 506/2004, un număr de **194 de notificări**, iar **sesizările** privind posibile neconformități cu dispozițiile Regulamentului (UE) 2016/679 s-au ridicat la un număr de **204**.



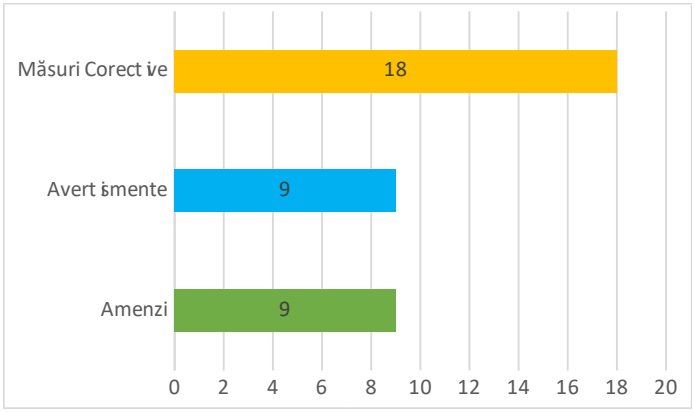
În ceea ce privește notificările încălcărilor de securitate, acestea au vizat în principal confidențialitatea/disponibilitatea/integritatea datelor cu caracter personal ca urmare a dezvăluirilor neautorizate ori ca urmare a unui software malițios (ransomware), accesul ilegal la datele cu caracter personal 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.

Sesizările primite au vizat, în principal lipsa măsurilor de securitate, inclusiv la nivelul website-urilor, publicarea/dezvăluirea datelor cu caracter personal în mediul on-line, în special pe rețelele de socializare.

Ca urmare a **sesizărilor primite și încălcărilor de securitate notificate** de către operatorii de date cu caracter personal, pe parcursul anului 2020, la nivelul Autorității naționale de supraveghere au fost demarate un număr de **398 de investigații din oficiu**.

În cadrul **investigațiilor efectuate din oficiu**, în anul 2020 au fost aplicate **9 amenzi** în cuantum total de **652.019,5 RON** (139.000 Euro), **9 avertismente** și **18 măsuri corective**.



Măsurile corective dispuse în urma plângerilor și a 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;
- 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;
- 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 în domeniul financiar-bancar

În domeniul financiar-bancar, investigațiile din oficiu 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 de către bănci, instituţii financiare nebancare, societăți de recuperări creanțe.

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.

În urma investigațiilor efectuate au fost aplicate atât sancțiuni contravenționale, cât și o serie de măsuri corective.

1. FIȘĂ DE CAZ – Divulgare neautorizată a datelor cu caracter personal ale unei persoane fizice (client) pe rețelele de socializare

O instituție bancară 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 prevăzut de Regulamentul (UE) 2016/679.

Astfel, instituția bancară ne-a informat cu privire la faptul că, în urma unei sesizări efectuată de către un client (terț de situație), a luat la cunoștință despre producerea unui incident de securitate, constând în dezvăluirea în spațiul public (on-line) a declarației solicitată de operator unui client al său cu privire la modul în care intenționa să utilizeze o anumită sumă de bani pe care acesta dorea să o ridice din contul său. Această declarație a fost distribuită între câțiva angajați ai băncii pe adresele de e-mail de serviciu. Unul dintre angajați a listat e-mailul ce conținea declarația clientului, precum și e-mailul ce conținea conversația internă între angajații operatorului. Un alt angajat a fotografiat cu telefonul mobil înscrisul listat și l-a distribuit prin intermediul aplicației WhatsApp. Ulterior, înscrisul listat a fost postat și distribuit pe rețeaua de socializare Facebook și pe un site.

Din investigația efectuată în acest caz, a rezultat că instituția bancară a încălcat prevederile art. 32 alin. (1) 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. Aceasta a condus la divulgarea neautorizată și accesul neautorizat la datele cu caracter personal (nume și prenume, adrese de e-mail, date comportamentale, preferințe personale, valoare tranzacție financiară, adresa locului de muncă, funcția și locul muncii, număr de telefon de serviciu) a 4 persoane fizice vizate (un client și 3 angajați proprii), prin dezvăluirea în spațiul public a unei conversații, prin intermediul poștei electronice (clasificată de „uz intern”) între angajații proprii, listată, fotografiată cu telefonul mobil și dezvăluită pe rețelele de socializare, deși potrivit art. 5 lit. f) din Regulamentul (UE) 2016/679, operatorul avea obligația de a respecta principiul „integritate și confidențialitate”.

Totodată, s-a constatat că dezvăluirea produsă probează ineficiența instruirii interne a angajaților operatorului privind obligațiile acestora referitoare la protecția

datelor cu caracter personal ale persoanelor vizate, inclusiv a măsurilor pe care operatorul era obligat să le ia, potrivit art. 32 alin. (4) din Regulamentul (UE) 2016/679, pentru a asigura faptul că orice persoană care acționează sub autoritatea sa nu prelucrează date cu caracter personal decât la cererea sa.

De asemenea, ca urmare a sesizării primite din partea persoanei vizate afectată de incidentul de securitate, Autoritatea națională de supraveghere a constatat că, dezvăluirea datelor cu caracter personal în spațiul public a generat o serie de prejudicii de natură morală, precum și alte dezavantaje semnificative de natură economică sau socială pentru aceasta.

În urma investigaţiei efectuate, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 487.380,00 lei (echivalentul a 100.000 EURO), pentru încălcarea prevederilor art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ - Divulgare neautorizată de date cu caracter personal ale clienților și angajaților prin intermediul e-mail-ului

O instituție bancară 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 prevăzut de Regulamentul (UE) 2016/679.

În fapt, adresele de e-mail ale angajaților și ale clienților unei instituții bancare (1332 persoane fizice) au fost dezvăluite neautorizat, ca urmare a completării, din eroare, a listei destinatarilor în câmpul CC (carbon copy), în loc de BCC (blind carbon copy). Astfel, adresele de e-mail individuale inserate în câmpul CC de către responsabilul desemnat cu trimiterea prin e-mail a raportului zilnic de analiză de piață către clienții societății abonați la newsletter, precum și către angajați ai unor societăți comerciale, au devenit vizibile tuturor destinatarilor mesajului.

Din investigația efectuată în acest caz, a rezultat că instituția bancară 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 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.

În urma investigaţiei efectuate, Autoritatea națională de supraveghere a aplicat măsura corectivă privind revizuirea şi actualizarea măsurilor tehnice şi organizatorice implementate ca urmare a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor 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 Regulamentul (UE) 2016/679, astfel încât să fie evitate incidente similare de dezvăluire neautorizată a datelor cu caracter personal prelucrate.

3. FIȘĂ DE CAZ – Prelucrarea de date cu caracter personal inexacte și dezvăluirea acestora către un partener contractual

O instituție bancară 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 prevăzut de Regulamentul (UE) 2016/679.

În fapt, instituția bancară a transmis către un partener contractual în vederea emiterii unor polițe de asigurare, două fișiere conținând atât informații corecte, cât și informații inexacte/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).

Din investigația efectuată în acest caz, a rezultat că, angajații departamentului de monitorizare al polițelor de asigurare 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 de către garanți 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 a producerii incidentului de securitate, instituția bancară a inițiat un proiect intern care are în vedere automatizarea procesului, simplificarea pașilor parcurși și includerea unor măsuri adiționale de verificare.

Totodată, Autoritatea națională de supraveghere a constatat că instituția bancară a încălcat prevederile art. 29, art. 32 alin. (2) și art. 32 alin. (4) din Regulamentul (UE) 2016/679 întrucât operatorul nu a luat suficiente măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea operatorului și care are acces la date cu caracter personal nu le prelucrează decât la cererea sa. 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 (referitoare la polițe care trebuiau emise) cât și informații inexacte/neactualizate.

În urma investigaţiei efectuate, 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.

4. FIȘĂ DE CAZ - prelucrare copii acte identitate ale persoanelor fizice (minori si reprezentanţi legali) și transmiterea acestora prin intermediul aplicaţiei WhatsApp

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că, în cadrul unei prezentări efectuată la o unitate școlară, angajata unei instituții bancare a prezentat un card de debit pentru încasarea burselor elevilor și a preluat prin intermediul telefonului personal, prin aplicația WhatsApp, în format electronic, poze cu copiile cărților de identitate ale copiilor și ale reprezentanților legali. Totodată, reprezentanta băncii a fotografiat cărțile de identitate ale persoanelor care nu aveau această aplicație instalată în telefon, ulterior transmițându-le pe adresa sa de e-mail de serviciu.

Din investigația efectuată în acest caz, a rezultat că instituția bancară nu a implementat măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de

securitate corespunzător riscului prelucrării, incluzând printre altele, după caz, capacitatea de a asigura confidenţialitatea, integritatea, disponibilitatea şi rezistenţa continue ale sistemelor şi serviciilor de prelucrare şi nu a luat măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea sa și are acces la date cu caracter personal nu le prelucrează decât la cererea sa, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern. Aceasta a condus la colectarea/prelucrarea copiilor actelor de identitate ale clienţilor persoanelor fizice (minori si reprezentanţi legali) prin intermediul telefonului personal al unei angajate şi/sau la transmiterea acestor copii prin intermediul aplicaţiei WhatsApp, cu încălcarea procedurilor de lucru.

Totodată, Autoritatea națională de supraveghere a constatat că, incidentul de securitate a afectat persoane vizate vulnerabile, respectiv minori, precum și faptul că datele cu caracter personal afectate de încălcare ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care prelucrarea poate conduce la furt sau fraudă a identităţii, pierdere financiară, pierderea confidenţialităţii datelor cu caracter personal protejate, sau la orice alt dezavantaj semnificativ de natură economică sau socială.

În urma investigaţiei efectuate, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 24.163,50 lei (echivalentul a 5000 EURO), pentru încălcarea prevederilor art. 32 alin. (1) lit. b) şi art. 32 alin. (4) din Regulamentul (UE) 2016/679.

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

Notificările încălcărilor de securitate în domeniul sănătății, precum și sesizările transmise Autorității naționale de supraveghere în cursul anului 2020, au vizat prelucrarea datelor cu caracter personal de către entități medicale din sectorul public (spitale). Acestea au avut ca obiect, în principal, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal ale persoanelor vizate (pacienți).

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

1. FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal ale pacienților de către o unitate spitalicească

O unitate spitalicească 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 prevăzut de Regulamentul (UE) 2016/679.

În fapt, dintr-o eroare a medicului curant, în camera de gardă a spitalului, au fost amestecate documente medicale aparținând a doi pacienți, ceea ce a condus la înmânarea acestor documente aparținătorului unuia dintre aceștia. Documentele medicale erau în format olograf și tipărite pe hârtie și card de plastic.

Categoriile de date cu caracter personal afectate de incidentul de securitate erau: nume și prenume, CNP, număr card de sănătate, număr foaie de observație, adresă, număr de telefon, informații privind starea de sănătate a persoanei vizate, informații referitoare la internare și locul de muncă.

La data efectuării investigației, Autoritatea națională de supraveghere a constatat că operatorul a prelucrat date cu caracter personal într-un mod care nu asigură securitatea adecvată, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare, în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal stocate sau prelucrate într-un alt mod. Aceasta a condus la divulgarea neautorizată de către un angajat propriu, a unor documente conținând date cu caracter personal de identificare (nume și prenume, CNP), număr card de sănătate, număr foaie de observație, date de contact (adresă, număr de telefon), date privind starea de sănătate, date privind internarea și date profesionale (locul de muncă) aparținând unui pacient, către un alt pacient al spitalului.

În urma investigației efectuate, Autoritatea națională de supraveghere a dispus împotriva operatorului, măsura corectivă privind revizuirea şi actualizarea măsurilor tehnice şi organizatorice implementate, 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, pentru încălcarea prevederilor art. 5 alin. (1) lit. f) și art. 32 alin. (2) din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ - Acces neautorizat la datele cu caracter personal ale unei paciente și ale copilului său

O unitate spitalicească 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 prevăzut de Regulamentul (UE) 2016/679.

În fapt, prin intermediul unei sesizări anonime, unitatea spitalicească a fost informată că o angajată din cadrul unei secții a avut acces neautorizat la datele cu caracter personal ale unei paciente și ale copilului său nou-născut.

La data efectuării investigației, Autoritatea națională de supraveghere a constatat că operatorul nu a luat măsuri pentru a asigura că orice persoană fizică care acționează sub autoritatea sa și are acces la date cu caracter personal nu le prelucrează decât la cererea sa, cu excepția cazului în care această obligație îi revine în temeiul dreptului Uniunii sau al dreptului intern și nu a implementat măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului prelucrării generat în special, în mod accidental sau ilegal, de divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal stocate sau prelucrate într-un alt mod. Aceasta a condus la accesarea foii de observație (date de contact, date de identificare, informații personale, informații medicale/sănătate și identificatori medicali) a unui nou născut în Secția Neonatologie a spitalului, de pe un cont de utilizator aparținând unui registrator medical din cadrul Secției Pediatrie.

În urma investigaţiei efectuate, pentru încălcarea prevederilor art. 32 alin. (4) raportat la art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679, Autoritatea națională de supraveghere a dispus împotriva operatorului, următoarele măsuri corective:

1. Efectuarea unei evaluări privind riscul pentru drepturile și libertățile persoanelor care să cuprindă inclusiv încadrarea într-un grad de risc, ținând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării.

2. Revizuirea şi actualizarea măsurilor tehnice şi organizatorice implementate ca urmarea a evaluării privind riscul pentru drepturile și libertățile persoanelor, inclusiv a procedurilor de lucru referitoare la protecția datelor cu caracter personal.

3. FIȘĂ DE CAZ – Dezvăluirea datelor cu caracter personal ale pacienților pe site-ul www.e-licitatie.ro

Autoritatea națională de supraveghere a fost sesizată cu privire la posibile încălcări ale legislației privind protecția datelor cu caracter personal, ca urmare a postării în Sistemul Electronic de Achiziții Publice (SEAP), pe site-ul www.e-licitatie.ro, de către o unitate spitalicească, a unor anunțuri de achiziții publice, care conțin date cu caracter personal ale pacienților minori (nume, prenume, date privind starea de sănătate).

Ca urmare a investigației efectuate, Autoritatea națională de supraveghere a constatat că nu a existat un temei legal al diseminării datelor cu caracter personal ale minorilor, pe site-ul www.e-licitatie.ro, în cadrul anunțurilor de achiziții publice postate în SEAP. Totodată, s-a constatat că, operatorul 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 prelucrate (nume, prenume, date de sănătate/analize medicale) ale pacienților minori pe site-ul www.e-licitatie.ro.

Unitatea spitalicească a fost sancționată contravențional cu avertisment, în temeiul art. 58 alin. (2) lit. b) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 15 alin. (1) din Legea nr. 102/2005, precum și în temeiul art. 12-14 din Legea nr. 190/2018, coroborate cu art. 7 din O.G. nr. 2/2001, întrucât 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 sau accesul neautorizat la datele cu caracter personal prelucrate (nume, prenume, analize medicale) ale pacienților minori, prin postarea unor anunțuri de achiziții publice, în SEAP, pe site-ul www.e-licitatie.ro.

Sancțiunea avertismentului a fost însoțită de aplicarea unei 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, 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.

C. Investigații la autorități și organisme publice

În anul 2020, investigațiile la autorități și organisme publice au fost efectuate, atât ca urmare a sesizărilor privind posibile încălcări ale prevederilor Regulamentului (UE) 2016/679, cât și ca urmare a notificărilor privind încălcarea securității datelor cu caracter personal transmise Autorității naționale de supraveghere.

Ca urmare a investigațiilor efectuate, au fost aplicate sancțiuni cu avertisment, însoțite de un plan de remediere. Totodată, au fost emise și două decizii de încetare a oricărei operațiuni sau set de operațiuni de prelucrare de date cu caracter personal și ștergerea sistemului de evidență a datelor cu caracter personal constituit ca urmare a unor astfel de prelucrări.

În majoritatea cazurilor, autoritățile și organismele publice au îndeplinit măsurile de remediere dispuse, în termenul acordat de Autoritatea națională de supraveghere

FIȘE DE CAZ – Prelucrare nelegală a datelor cu caracter personal prin utilizarea unor sisteme de supraveghere audio-video portabile în activitatea polițiștilor locali

1. Autoritatea națională de supraveghere a fost sesizată referitor la obligația polițiștilor locali din cadrul unei structuri de a purta asupra lor camere de înregistrare audio-video, având încorporată și funcția de GPS (Global Positioning System), pornite pe întreaga durată a desfășurării activității.

În cadrul investigației desfășurate de către Autoritatea națională de supraveghere, operatorul a declarat că scopul utilizării sistemelor de supraveghere audio — video este protecția polițiștilor locali împotriva faptelor de ultraj și a acuzațiilor îndreptate împotriva acestora cu privire la modul de exercitare a atribuțiilor de serviciu, 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. Totodată, s-a menționat că sistemul audio-video portabil este prevăzut cu GPS (Global Positioning System), inactiv din fabricație.

La data efectuării investigației, operatorul nu a putut face dovada respectării privind legalitatea prelucrării efectuate prin intermediul sistemului audio-video portabil de tip ”Body-Worn Camera”, în contextul obligativității impuse polițiștilor locali, de a purta asupra lor, în timpul programului de lucru, mijloace de supraveghere audio – video, precum și faptul că temeiurile legale invocate nu conțin dispoziții care să reglementeze utilizarea unor astfel de sisteme, în general, și nici utilizarea sistemelor audio-video portabile în activitatea polițiștilor locali.

Autoritatea publică a fost sancționată contravențional cu avertisment, în temeiul art. 58 alin. (2) lit. b) din Regulamentul (UE) 2016/679, raportat la art. 14 alin. (11) și art. 15 alin. (1) din Legea nr. 102/2005, precum și în temeiul art. 12-14 din Legea nr. 190/2018, coroborate cu art. 7 din O.G. nr. 2/2001, întrucât personalul propriu, aflat în exercitarea misiunilor și activităților specifice, a prelucrat date cu caracter personal prin utilizarea sistemului audio-video portabil de tip ”Body-Worn Camera” (care prelucrează imaginea și vocea), fără să existe o obligaţie legală a operatorului și fără îndeplinirea vreunei alte condiții prevăzute la art. 6 alin. (1) din Regulamentul (UE) 2016/679, deși 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 persoana vizată.

Sancțiunea avertismentului a fost însoțită de aplicarea unei măsuri corective, prin planul de remediere, potrivit dispozițiilor art. 12- 14 din Legea nr. 190/2018. Astfel, în sarcina operatorului s-a dispus asigurarea conformității operațiunilor de prelucrare, efectuate prin utilizarea sistemelor audio-video portabile de tip ”Body-Worn Camera”, cu dispozițiile art. 5 și art. 6 din Regulamentul (UE) 2016/679.

Totodată, Autoritatea națională de supraveghere a dispus, prin Decizie, încetarea oricărei operațiuni sau set de operațiuni de prelucrare de date cu caracter personal efectuată prin intermediul sistemelor audio-video portabile și șteargerea sistemului de evidență a datelor cu caracter personal constituit ca urmare a utilizării unor astfel de sisteme.

2. Ca urmare a unei sesizări cu privire la încălcarea legislației privind protecția datelor cu caracter personal referitor la obligația polițiștilor locali din cadrul unei structuri de poliție locală de a purta asupra lor, în timpul programului de lucru, camere de înregistrare audio – video, Autoritatea națională de supraveghere a constatat că, operatorul investigat prelucrează date cu caracter personal prin intermediul unor mijloace de supraveghere audio - video portabile, de tip „BADGE", utilizate de către personal în misiuni și activități derulate pe teren, în contextul în care polițiștilor locali le-a fost stabilită ierarhic obligația de a purta asupra lor, în timpul programului de lucru aceste mijloace de supraveghere audio — video.

În cadrul investigației desfășurate, operatorul a declarat că scopul prelucrării îl reprezintă îndeplinirea obligațiilor legale ce-i revin în vederea îndeplinirii sarcinilor care servesc intereselor publice și care rezultă din exercitarea autorității publice cu care această instituție este învestită, fiind reglementate modalitățile de utilizare a mijloacelor de supraveghere video de acest tip în misiuni și activități, în teren, în spații deschise, pentru documentarea/imortalizarea pe suport electronic a faptelor care constituie contravenții sau infracțiuni precum și pentru înregistrarea pe suport electronic a cazurilor de ultraj.

Operatorul a indicat drept temei legal Regulamentul (UE) 2016/679 și legislația națională de transpunere a Directivei (UE) 216/680 a Parlamentului European și a Consiliului din 27.04.2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente, în scopul prevenirii, depistării, investigării penale a infracțiunilor, sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-Cadru 2008/977/JAI a Consiliului, publicată în Jurnalul Oficial al Uniunii Europene, seria L nr. 119/04.05.2016, în vederea prevenirii și combaterii săvârșirii infracțiunilor, supravegherea traficului rutier și constatarea încălcării regulilor de circulație rutieră, îndeplinirea unor măsuri de interes

public, exercitarea prerogativelor de autoritate publică sau realizarea unui interes legitim, precum și reglementările interne.

Totodată, operatorul mai precizează că obiectivele camerelor de înregistrare audio-video sunt orientate către persoanele care săvârșesc acte antisociale ori către persoanele aflate în dificultate și care necesită acordarea ajutorului de urgență; mijloacele de supraveghere implementate permit înregistrarea audio-video și mărirea sau micșorarea imaginilor după finalizarea operațiunilor de descărcare, nefiind posibilă alterarea imaginilor și sunetelor captate în scopul falsificării acestora, iar informarea prealabilă a contravenientului/contravenienților/persoanelor aflate în dificultate, cu privire la faptul că întreaga procedură acțională este supusă înregistrării audio-video, este realizată de polițiștii locali aflați în exercitarea atribuțiilor de serviciu; stocarea imaginilor se realizează pe echipamente de stocare protejate și nu pot fi accesate decât de pe echipamente dedicate, destinatarii datelor sunt conducătorul instituției, persoanele abilitate în efectuarea activității de control și alte structuri la solicitare.

Din investigația efectuată în acest caz, s-a constatat că nu există dispoziții legale care să reglementeze utilizarea unor sisteme de supraveghere audio — video portabile în activitatea polițiștilor locali.

Ca atare, s-a constatat că prelucrarea datelor cu caracter personal (imagine, voce) s-a efectuat fără îndeplinirea condițiilor de legalitate a prelucrării, așa cum sunt prevăzute în art. 6 alin. (1) din Regulamentul (UE) 2016/679. Precizăm că, 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 avertisment, însoțit de măsura inclusă în 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.

Urmare a constatărilor prin procesul-verbal de constatare/sancționare și având în vedere că operatorul încetase prelucrarea datelor cu caracter personal prin astfel de sisteme, Autoritatea națională de supraveghere a dispus, prin decizie, ștergerea datelor cu caracter personal din sistemul de evidență constituit ca urmare a utilizării sistemelor audio-video.

FIȘĂ DE CAZ – Divulgarea neautorizată a datelor cu caracter personal pe o rețea de socializare

Prin transmiterea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679, o autoritate publică a notificat Autoritatea națională de supraveghere cu privire la faptul că o listă (borderou) privind acordarea de ajutor de urgență pentru sprijinirea familiilor afectate de inundații, întocmită în cadrul autorității respective, a fost postată pe o rețea de socializare (Facebook), într-un grup privat cu 700 de membri. Lista conținea datele cu caracter personal ale unui număr de 45 de beneficiari ai ajutorului de urgență: nume, prenume beneficiari, adresă, grad de afectare a locuinței, CNP, suma propusă pentru ajutor. În urma investigației efectuate de către Autoritatea națională de supraveghere, s-a constatat că autoritatea publică în cauză a încălcat prevederile art. 32 alin. (1) lit. b) și alin. (2) din Regulamentul (UE) 2016/679, întrucât 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 a datelor cu caracter personal, transmise, stocate sau prelucrate într-un alt mod sau accesul neautorizat la aceste date. Aceasta a condus la divulgarea neautorizată a datelor cu caracter personal a 45 persoane fizice vizate, prin postarea pe rețeaua de socializare a listei (borderou) privind acordarea de ajutor de urgență pentru sprijinirea familiilor afectate de inundații.

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, Autoritatea națională de supraveghere a aplicat măsura corectivă privind instruirea angajaților asupra riscurilor și consecințelor pe care le implică divulgarea datelor personale.

D. Investigații în alte cazuri

În general, încălcările de securitate a datelor cu caracter personal notificate de către entitățile din domeniul privat au avut ca obiect 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.

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

1. FIȘĂ DE CAZ – Divulgarea neautorizată de date cu caracter personal prin intermediul platformei informatice utilizate pentru înscrierea participanților la evenimente

Prin completarea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679, o societate comercială a notificat Autoritatea națională de supraveghere cu privire la divulgarea neautorizată a datelor cu caracter personal ale participanților la un eveniment, din cauza unei erori tehnice. În fapt, din cauza unei erori tehnice, cu ocazia organizării unui eveniment, operatorul investigat a realizat o trimitere defectuoasă de e-mail-uri, de pe platforma utilizată în acest scop, către un număr de aproximativ 1300 persoane fizice, utilizatori ai platformei. Astfel, adresa de e-mail, numele de utilizator și user-ul pentru logarea pe platforma de eveniment on-line au fost transmise altor persoane decât titularilor, în mod eronat. La data efectării investigației, Autoritatea națională de supraveghere a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului 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. Aceasta a condus la divulgarea și accesul neautorizat la datele cu caracter personal ale unui număr de 1300 utilizatori, în urma rulării unui script, prin care a fost efectuată conversia greșită a formatului Excel.

În urma investigaţiei efectuate, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 9.671,40 lei (echivalentul a 2000 EURO), pentru încălcarea prevederilor art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679 coroborat cu art. 5 alin. 1 lit. f) din Regulamentul (UE) 2016/679.

2. FIȘĂ DE CAZ - Accesul neautorizat și divulgarea neautorizată a datelor cu caracter personal prin postarea codului sursă al website-lui

Prin completarea formularului privind încălcarea securității datelor cu caracter personal prevăzut de Regulamentul (UE) 2016/679, o companie de vânzări auto a notificat Autoritatea națională de supraveghere referitor la accesul neautorizat și divulgarea neautorizată a datelor cu caracter personal ale clienților, prin postarea pe pagina de Facebook a societății, a unui document cu o captură din codul sursă al website-ului pe care compania a desfășurat un concurs on-line de atragere a clienților participanți în service-ul auto.

În fapt, dintr-o eroare tehnică, în codul sursă postat pe pagina de Facebook a societății, era inclusă și parola de acces la formularele completate de participanții la concurs. Extragerea și utilizarea parolei din codul sursă a condus la vizualizarea datelor cu caracter personal ale unui număr de 436 clienți ai companiei de vânzări auto (nume și prenume, localitate, telefon, e-mail, autoturism deținut și serie de șasiu).

La data efectuării investigației, Autoritatea națională de supraveghere a constatat că operatorul investigat 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, stocate sau prelucrate într-un alt mod. Aceasta a condus la accesul neautorizat la datele cu caracter personal (nume și prenume, localitate, telefon, e-mail, autoturism deținut și serie de șasiu) ale unui număr de 436 clienți ai companiei, pe website-ul acesteia, și la divulgarea neautorizată a acestor date.

În urma investigaţiei efectuate, Autoritatea națională de supraveghere a sancționat operatorul cu amendă în cuantum de 72.642,00 lei (echivalentul a 15.000 EURO), pentru încălcarea prevederilor art. 32 alin. (1) și alin. (2) din Regulamentul (UE) 2016/679.

Totodată, s-a dispus măsura corectivă privind 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, astfel încât să fie evitate incidente similare de dezvăluire neautorizată a datelor cu caracter personal prelucrate.

Secţiunea a 3 -a: Activitatea de soluţionare a plângerilor

I. Prezentare generală

În cursul anului 2020, la Autoritatea naţională de supraveghere au fost înregistrate, analizate şi soluţionate plângeri legate de prelucrarea datelor cu caracter personal care intră sub incidenţa Regulamentului (UE) 679/2016, aplicabil din 25 mai 2018, și a legislației naționale de implementare a prevederilor acestuia, respectiv Legea nr. 102/2005, republicată, precum și Legea nr. 190/2018, sau a altor dispoziţii legale aplicabile în domeniul protecţiei dreptului la viaţă intimă, familială şi privată prin prelucrarea datelor personale, inclusiv în sectorul comunicaţiilor electronice şi al comerţului electronic.

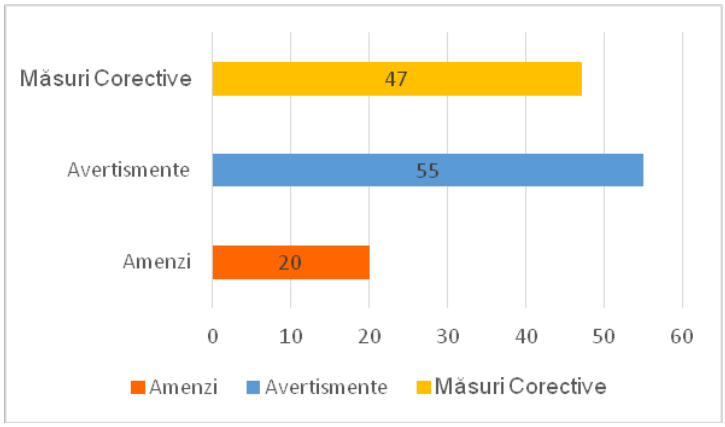
Autoritatea naţională de supraveghere a primit, în anul 2020, un număr total de **5082** plângeri, pe baza cărora au fost demarate **296** de investigații.

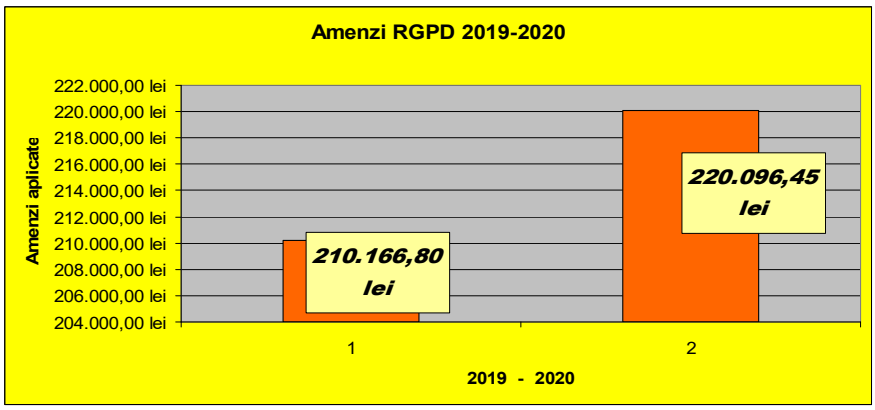
În anul 2020, plângerile primite de Autoritatea naţională de supraveghere au vizat, în principal, următoarele:

- 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.

Urmare a investigațiilor efectuate pe baza plângerilor, au fost aplicate următoarele sancţiuni contravenţionale :

- **20 amenzi**, dintre care 18 în baza Regulamentului (UE) 2016/679, în cuantum total de 220.096,45 lei (echivalentul sumei de 45.500 Euro) și 2 amenzi în baza Legii nr. 506/2004, în cuantum total de 20.000 lei;
- **55 de avertismente**;
- **47 măsuri corective** în baza dispozițiilor art. 58 alin. (2) lit. c) și d) din Regulamentul (UE) 2016/679.





Măsurile corective aplicate de Autoritatea naţională de supraveghere au vizat, în 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;

❖ Instruirea persoanelor care prelucrează date sub autoritatea operatorului (angajații operatorului);

❖ Efectuarea de verificări periodice în sistemul propriu de evidență în vederea verificării corectitudinii datelor colectate, în scopul evitării prelucrării ilegale.

În majoritatea cazurilor investigate, operatorii au implementat măsurile dispuse de Autoritatea națională de supraveghere astfel încât să fie respectate reglementările în vigoare în materia protecției datelor personale.

De asemenea, în anul 2020, Autoritatea naţională de supraveghere a primit o serie de plângeri care nu au putut fi considerate admisibile și, pe cale de consecință, nu au format obiectul unor demersuri de investigare. Principalele motive pentru care plângerile menționate mai sus au fost considerate inadmisibile au fost următoarele:

- lipsa furnizării datelor de identificare ale petenților;
- lipsa dovezilor în susţinerea aspectelor reclamate;
- sesizarea unor aspecte care nu intră în competența legală materială a Autorității naționale de supraveghere (de ex. aspecte care țin de aplicarea legislației din domeniul dreptului penal sau al protecției drepturilor consumatorilor);
- imposibilitatea determinării aspectelor care formează obiectul petiției.

În același timp, o serie de plângeri au fost considerate neîntemeiate ca urmare a faptului că petenții și-au bazat nemulțumirea pe lipsa consimțământului lor pentru prelucrarea datelor, fără a lua în considerare existența și a altor temeiuri legale de prelucrare a datelor, care nu necesită obținerea de către operatorul de date a

consimțământului persoanei vizate (ex. prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului) sau că există situații în care operatorii nu au obligația de a da curs cererilor de exercitare a drepturilor persoanelor vizate (ex. persoana vizată nu va obține ștergerea datelor în măsura în care prelucrarea este necesară pentru exercitarea dreptului la liberă exprimare şi la informare sau pentru respectarea unei obligaţii legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului).

II. Principalele constatări rezultate din activitatea de soluționare a plângerilor

În această secțiune vor fi prezentate o serie de cazuri în care investigațiile efectuate pentru soluționarea plângerilor admisibile primite de Autoritatea națională de supraveghere au fost finalizate pe parcursul anului 2020 prin aplicarea unor sancțiuni contravenționale, respectiv, a unor măsuri corective împotriva operatorilor reclamați, atât din sectorul public, cât și din sectorul privat.

1. Investigații referitoare la nerespectarea drepturilor persoanelor vivate

Regulamentul (UE) 2016/679 a consolidat drepturile garantate persoanelor vizate, punându-se accent pe modalităţile de exercitare a acestor drepturi.

În acest context, operatorii de date cu caracter personal trebuie să stabilească modalităţi de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin Regulament, inclusiv mecanismele prin care aceasta poate solicita şi, dacă este cazul, obţine, în mod gratuit, în special, acces la datele cu caracter personal, precum şi rectificarea sau ştergerea acestora, şi exercitarea dreptului la opoziţie. De asemenea, operatorii trebuie să ofere modalităţi de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice.

În acelaşi timp, operatorii trebuie să respecte obligaţia de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate şi cel târziu în termen de o lună şi, în cazul în care nu intenţionează să se conformeze respectivelor cereri, să motiveze acest refuz.

În anul 2020, nerespectarea drepturilor persoanelor vizate a constituit obiectul multor plângeri adresate Autorității naționale de supraveghere.

Astfel, ca urmare a investigaţiilor efectuate, s-a constatat faptul că unii operatori de date cu caracter personal nu au soluţionat cererile adresate de persoanele vizate 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 modalităţi concrete de exercitare a drepturilor persoanelor vizate.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că un operator nu a răspuns la cererea prin care petentul solicita ștergerea datelor sale, ca urmare a faptului că figura în baza de date ca persoană de contact pentru un alt abonat al operatorului, fără acordul său, aspect de care a luat cunoștință cu ocazia unui apel telefonic din partea unui angajat al acestuia. Petentul a menționat că nu cunoaște persoana în cauză și nici nu a avut relații juridice cu operatorul. Prin cererea sa, petentul a solicitat ștergerea informațiilor legate de nume, prenume și număr de telefon, precum și orice alte informații deținute de operator cu privire la persoana sa, inclusiv sursa de colectare a datelor.

În cadrul investigației efectuate în acest caz, s-a constatat că operatorul a colectat numărul de telefon al petentului de la o altă persoană (nenominalizată), în condițiile în care acesta nu este client al operatorului și nu îl cunoștea pe abonatul care i-a declarat numărul ca dată de contact. Operatorul nu a făcut dovada că a dat curs cererii de ștergere a datelor petentului, conform solicitării acestuia și nici că a transmis un răspuns la cererile prin care își exercita drepturile de acces și de ștergere.

Întrucât acest operator nu era la prima abatere constatată în baza Regulamentului (UE) 2016/679, s-a dispus sancționarea cu amendă și aplicarea unei măsuri corective (comunicarea unui răspuns către petent), pentru încălcarea art. 12, 15 și 17 din Regulamentul (UE) 2016/679.

FIȘĂ DE CAZ

Un petent a sesizat faptul că o instituție de credit i-a încălcat dreptul de opoziție, în contextul în care, ulterior exercitării acestui drept cu privire la prelucrarea datelor sale în scop de marketing, i-a transmis un mesaj comercial pe adresa sa de e-mail.

Din investigația efectuată, a reieșit că petentul și-a furnizat datele, respectiv adresa de e-mail, la deschiderea relației contractuale cu banca. Ca urmare a exercitării dreptului de opoziție cu privire la prelucrarea datelor sale pentru transmiterea de comunicări comerciale, în evidențele băncii petentul figura că nu și-a exprimat consimțământul pentru prelucrarea datelor sale în scop de marketing direct.

Cu toate acestea, ulterior acestor modificări, petentului i-a fost transmis un mesaj comercial pe adresa sa de e-mail, din cauza unei erori operaționale privind modul de adresare și contactare a clienților băncii. Această eroare a fost remediată de operatorul de date, iar adresa de e-mail a petentului a fost eliminată din evidențele băncii.

Față de constatări, operatorul a fost sancționat contravențional cu avertisment pentru încălcarea prevederilor art. 21 din Regulamentul (UE) 2016/679, deoarece avea obligația de a nu mai prelucra datele persoanei vizate în scop de marketing direct, în cazul în care aceasta s-a opus prelucrării datelor sale în acest scop.

De asemenea, a fost dispusă o măsura corectivă, operatorul având obligația de a adopta măsurile necesare în vederea respectării drepturilor persoanelor vizate, prin raportare la cerințele art. 21 din Regulamentul (UE) 2016/679 și cu respectarea prevederilor art. 7 din același Regulament.

FIȘĂ DE CAZ

Un petent a sesizat primirea pe adresa sa de e-mail a unui mesaj din partea operatorului reclamat (ce deținea un site de vânzări on-line), deși solicitase anterior să fie dezactivată din baza de date opțiunea de trimitere a unor astfel de mesaje prin e-mail, conform setărilor contului său de client, fiindu-i confirmată dezabonarea de la comunicările comerciale trimise de societate.

Operatorul reclamat mai fusese sancționat contravențional cu avertisment, ca urmare a plângerii aceluiași petent, pentru încălcarea dispozițiilor referitoare la dreptul de opoziție, dispunându-se măsurile corective de a se lua în considerare solicitarea

petentului de a-i fi dezactivată din baza de date setarea privind transmiterea pe adresa de e-mail a mesajelor referitoare la chestionarele de satisfacție și de a lua măsuri astfel încât să fie respectate, în toate cazurile, prevederile art. 21 din Regulamentul (UE) 2016/679.

Ca urmare a investigației efectuate, s-a constatat că operatorul a încălcat prevederile art. 6 din Regulamentul (UE) 2016/679, referitoare la legalitatea prelucrării, prin raportare la dispozițiile art. 21 alin. (3) din același Regulament, fiind sancționat contravențional cu amendă și reiterându-se măsurile corective dispuse anterior.

2. Investigații referitoare la încălcarea regulilor de confidențialitate și securitate a prelucrărilor de date

Una dintre principalele obligații ale operatorilor de date personale și ale persoanelor împuternicite de operatori prevăzute de Regulamentul (UE) 2016/679 se referă la implementarea unor măsuri adecvate şi eficace, precum şi la posibilitatea de a demonstra conformitatea activităţilor de prelucrare cu acest Regulament, inclusiv eficacitatea măsurilor. Aceste măsuri ar trebui să ţină seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscul pentru drepturile şi libertăţile persoanelor fizice.

Printre prelucrările de date cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală astfel încât să determine un risc pentru drepturile şi libertăţile persoanelor fizice, Regulamentul (UE) 2016/679 enumeră, în special, cazurile în care: prelucrarea poate conduce la discriminare, furt sau fraudă a identităţii, pierdere financiară, compromiterea reputaţiei, pierderea confidenţialităţii datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială; sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situaţia economică, starea de sănătate, preferinţele sau interesele personale, fiabilitatea sau comportamentul, locaţia sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal şi afectează un număr larg de persoane vizate.

Ca urmare a faptului că anumiţi operatori de date cu caracter personal nu au implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător prelucrărilor de date efectuate, în anul 2020, Autoritatea naţională de supraveghere a înregistrat o serie de plângeri care au avut ca obiect atât dezvăluirea datelor personale către terțe persoane, cât și accesarea neautorizată a datelor personale ale persoanelor vizate.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că pe un site prin intermediul căruia se comercializau anumite produse puteau fi vizualizate datele personale ale clienților respectivei societăți. Cu toate că petentul a adus la cunoștința operatorului aceste aspecte, nu a primit niciun răspuns, problema semnalată nefiind remediată.

În cadrul investigației efectuate în acest caz, a rezultat că, urmare a unor erori de sincronizare a drepturilor de utilizator, comisă în cursul scrierilor de coduri sursă la momentul construirii site-ului respectiv, au apărut disfuncționalități care au făcut posibilă accesarea și vizualizarea unor date personale aparținând clienților acestei societăți. Astfel, după logarea în contul de utilizator, era posibilă vizualizarea unor comenzi conținând datele personale ale altor clienți (adresă e-mail, nume, prenume, număr de telefon, adresă, produse comandate, preț, date de livrare și facturare). Operatorul a declarat că nu a cunoscut problema ce i-a fost semnalată de petent, susținând că mesajul acestuia ar fi fost salvat în secțiunea de *spam* din serviciul de poștă electronică folosit. Ca atare, a luat la cunoștință de aceste erori doar în cadrul investigației demarate de Autoritatea națională de supraveghere și a luat măsuri de remediere în aceeași zi. Totodată, a notificat Autoritatea națională de supraveghere cu privire la incidentul de securitate produs și a trimis un răspuns către petent.

Prin urmare, s-a reținut faptul că operatorul nu a adoptat suficiente măsuri de securitate încă din momentul conceperii site-ului, care să prevină accesarea și divulgarea neautorizată a datelor personale ale clienților care au plasat comenzi pe acest site.

În consecință, s-a dispus sancționarea contravențională cu amendă a operatorului, pentru încălcarea art. 25 și 32 din Regulamentul (UE) 2016/679.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că o companie de furnizare energie electrică a încălcat securitatea și confidențialitatea datelor cu caracter personal prin transmiterea unor documente ce conțineau datele personale ale petentului unui alt client al societății, prin intermediul poștei electronice.

În vederea încheierii unui nou contract de furnizare a energiei electrice, la solicitarea operatorului, petentul a transmis acestuia, prin poșta electronică, o serie de înscrisuri care conțineau datele sale cu caracter personal. Din eroare, agentul care a recepționat corespondența, în loc să o trimită pentru a fi procesată, analizată și pentru a i se răspunde petentului, a trimis către o adresă de e-mail a unui alt client, care a informat petentul referitor la dezvăluirea datelor sale personale.

Petentul a susținut, de asemenea, că a semnalat aceste aspecte și operatorului, însă nu a primit un răspuns.

Ca urmare a investigației efectuate, s-a constatat că operatorul a încălcat prevederile art. 32 din Regulamentul (UE) 2016/679, întrucât nu a făcut dovada asigurării confidenţialităţii datelor cu caracter personal, făcând posibilă dezvăluirea unor documente care conțineau datele cu caracter personal aparținând petentului.

Față de constatări, operatorul a fost sancționat contravențional cu amendă și s-a dispus măsura corectivă de a se adopta măsuri adecvate și eficiente de securitate, atât din punct de vedere tehnic, cât și din punct de vedere organizatoric.

FIȘĂ DE CAZ

Printr-o petiție transmisă la Autoritatea națională de supraveghere, o persoană fizică a reclamat faptul că o societate care are ca obiect principal de activitate instalarea, furnizarea și distribuția de gaze a transmis prin e-mail o ”Notificare de schimbare încadrare consumator și schimbare preț” către mai multe persoane, dezvăluind astfel adresele de e-mail ale acestora.

În cadrul investigației efectuate, s-a constatat că operatorul nu a adoptat suficiente măsuri de securitate pentru a asigura confidențialitatea datelor personale ale clienților săi, conform obligațiilor impuse de art. 32 din Regulamentul (UE) 2016/679, fapt ce a rezultat în trimiterea unei notificări către adresele de poștă electronică aparținând unui

număr de 19 clienți (persoane fizice), fără ascunderea acestora (eventual, prin folosirea funcției ”BCC”-”blind carbon copy”), permițând astfel divulgarea neautorizată a adreselor de e-mail către ceilalți destinatari. Cu toate că a invocat o eroare a sistemului informatic, care ar fi generat transmiterea respectivei corespondențe, operatorul nu a probat acest aspect.

În consecință, s-a dispus sancționarea contravențională a operatorului, pentru încălcarea art. 32 din Regulamentul (UE) 2016/679, precum și o măsură corectivă, în sensul de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de prelucrare a datelor personale, prin implementarea unor măsuri tehnice și organizatorice adecvate în cazul transmiterii la distanță a datelor personale, inclusiv sub aspectul instruirii regulate a persoanelor care prelucrează date sub autoritatea sa (angajați sau colaboratori).

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la utilizarea frauduloasă a datelor personale ale petentului la încheierea unor contracte de furnizare servicii de telefonie.

Urmare a efectuării investigației, s-a constatat că, în cadrul demersurilor efectuate de o altă persoană decât petentul, finalizate prin încheierea pe numele său a unui contract pentru două abonamente de servicii de telefonie mobilă, cu achiziție de echipamente, operatorul nu a făcut dovada adoptării unor măsuri de securitate și confidențialitate suficiente pentru protejarea datelor personale ale petentului. Astfel, s-a constatat, printre altele, că, în cadrul convorbirii telefonice, angajații/colaboratorii operatorului au furnizat persoanei apelante respective, la solicitarea acesteia, codul de abonat al petentului, care a fost folosit ulterior în mod fraudulos în convorbirile succesive care au avut ca rezultat încheierea contractelor pe numele petentului. Alte aspecte constatate au fost în legătură cu procedura sumară de identificare/autentificare a persoanei apelante, folosită în cadrul interacțiunilor telefonice, iar modul în care acestea au avut efectiv loc denotă un nivel insuficient de instruire a angajaților/colaboratorilor operatorului în privința respectării regulilor de confidențialitate și protecție a datelor personale ale clienților.

În urma investigației, pentru încălcarea dispozițiilor art. 32 din Regulamentul (UE) 2016/679, au fost aplicate o amendă și o măsură corectivă constând în obligarea operatorului la implementarea unor proceduri eficiente de identificare a persoanelor, care să prevină prelucrarea ilegală a datelor personale și dezvăluirea lor neautorizată, atât de către angajații/colaboratorii operatorului, cât și de către persoanele împuternicite și angajații/colaboratorii acestora, instruirea regulată a acestora și verificarea periodică a respectării instrucțiunilor date.

3. Investigații referitoare la prelucrarea datelor personale ale angajaților

În conformitate cu prevederile art. 5 din Legea nr. 190/2018, prelucrarea datelor agajaților la locul de muncă prin utilizarea sistemelor de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video, în scopul realizării intereselor legitime urmărite de operator, este permisă numai cu îndeplinirea anumitor condiții strict reglementate.

Astfel, în cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaţilor, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă:

- interesele legitime urmărite de angajator sunt temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;
- angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;
- angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;
- alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu şi-au dovedit anterior eficienţa; şi
- durata de stocare a datelor cu caracter personal este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

În acest context, întrucât sistemele de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video comportă anumite riscuri în privinţa drepturilor şi libertăţilor acestor categorii de persoane vulnerabile, precum angajații, înainte de instalarea unor astfel de sisteme de supraveghere, angajatorul trebuie să facă în prealabil o evaluare a riscurilor la care se supune activitatea sa pentru a stabili necesitatea implementării lor.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că pe mașinile de serviciu utilizate de o clinică medicală au fost instalați senzori Global Positioning System (GPS) și că se prelucrează astfel date personale, fără ca angajații să fi fost informați cu privire la drepturile lor în acest context.

În cadrul investigației efectuate în acest caz, operatorul a declarat că instalarea sistemului de localizare prin GPS pe mașinile societății corespunde unui interes legitim, pentru realizarea următoarelor scopuri: monitorizarea numărului de kilometri și prevenirea depășirii acestora având în vedere numărul de kilometri asumați pentru fiecare autoturism prin contractul de leasing operațional, optimizarea procesului de muncă, probarea vinovăției/nevinovăției utilizatorilor auto în cazul unor incidente reclamate de terți, facilitarea intervenției în cazul producerii unui accident în zone izolate și prevenirea furtului autovehiculului.

Cu toate acestea, din documentele puse la dispoziție de operator, nu a rezultat dacă, anterior luării deciziei de instalare și utilizare a sistemului de monitorizare prin GPS, s-a încercat utilizarea altor metode mai puțin intruzive, pentru atingerea acelorași scopuri și care să-și fi dovedit anterior ineficiența, așa cum prevede art. 5 din Legea nr. 190/2018. De asemenea, operatorul nu a prezentat dovezi din care să rezulte că a realizat o consultare prealabilă a sindicatului sau a reprezentanților angajaților înainte de introducerea acestui sistem de monitorizare, și nici o informare prealabilă, completă și explicită a acestora, așa cum prevede art. 5 din Legea nr. 190/2018. Totodată, s-a constatat că operatorul stoca datele care proveneau din folosirea sistemului de monitorizare prin GPS pentru 12 luni, fără să prezinte dovezi din care să rezulte că

depășirea termenului de 30 de zile prevăzut de art. 5 din Legea nr. 190/2018 se baza pe motive justificate.

Pe baza acestor constatări, s-a dispus aplicarea a două sancțiuni contravenționale și a două măsuri corective, pentru încălcarea dispozițiilor art. 5 din Legea nr. 190/2018, prin raportare la art. 5 și 6 din Regulamentul (UE) 2016/679. Prin cele două măsuri corective, s-a impus operatorului obligația de a asigura conformitatea cu Regulamentul (UE) 2016/679 a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin reevaluarea necesității atingerii scopurilor propuse prin folosirea datelor de localizare provenite din sistemul de monitorizare prin GPS instalate pe mașinile de serviciu ale angajaților operatorului, precum și prin limitarea perioadei de stocare a datelor prin raportare la scopurile prelucrării datelor, conform obligațiilor prevăzute de Regulamentul (UE) 2016/679 și de Legea nr. 190/2018.

4. Investigații referitoare la prelucrarea datelor personale de către asociațiile de proprietari

În anul 2020, o parte din plângerile adresate Autorității naţionale de supraveghere au avut ca obiect prelucrarea nelegală a datelor cu caracter personal de către asociațiile de proprietari, fie prin afișarea la avizierul condominiului a diferite documente care conțineau date cu caracter personal ale proprietarilor, fie prin utilizarea imaginilor video ale acestora în alt scop decât cel pentru care au fost instalate inițial camerele de supraveghere la nivelul asociației de proprietari.

FIȘĂ DE CAZ

Printr-o plângere trimisă la Autoritatea națională de supraveghere, o persoană fizică a reclamat accesarea, utilizarea și dezvăluirea fără temei legal a unor imagini cu persoana sa, provenite din sistemul de supraveghere video al asociației de proprietari a blocului în care locuiește. Petentul a atașat mai multe fotografii din care rezulta dezvăluirea unor astfel de imagini.

În cadrul investigației efectuate, operatorul a declarat că vandalizarea avizierului asociației prin distrugerea unor documente de la avizier și dispariția unor magneți de fixare sunt circumstanțele care au condus la accesarea imaginilor din sistemul de

supraveghere video al asociației, ce îl surprind pe petent și dezvăluirea ulterioară a acestora prin afișare în holul imobilului.

Astfel, s-a constatat că imaginea petentului a fost folosită într-un mod incompatibil cu scopul pentru care au fost instalate inițial camerele de supraveghere la nivelul asociației de proprietari, cu încălcarea principiilor și a condițiilor de legalitate a prelucrării prevăzute de art. 5 și 6 din Regulamentul (UE) 2016/679.

De asemenea, s-a reținut că operatorul nu a adoptat măsuri tehnice și organizatorice adecvate pentru protejarea datelor personale colectate prin intermediul sistemului de supraveghere video, inclusiv sub aspectul amplasării monitorului în holul de la parter, imaginile de pe acesta fiind vizibile pentru orice persoană care are acces în imobil (locatari, vizitatori, etc.), precum și al accesării imaginilor de la distanță prin internet, astfel încât să se evite accesarea, diseminarea sau prelucrarea în mod neautorizat a datelor personale prin intermediul acestui sistem.

În plus, nu au fost prezentate dovezi din care să rezulte că operatorul a asigurat informarea completă a persoanelor vizate ale căror date personale le prelucrează (imaginea), prin intermediul sistemului de supraveghere video, instalat în anul 2019, care funcționa și la data investigației.

Prin urmare, au fost aplicate sancțiuni contravenționale, inclusiv sub forma unei amenzi, și s-au dispus două măsuri corective, după cum urmează:

- adoptarea unor măsuri de securitate, tehnice și organizatorice, adecvate pentru protejarea datelor personale colectate prin intermediul sistemului de supraveghere video, inclusiv sub aspectul vizualizării imaginilor prin intermediul monitorului amplasat în holul de trecere (acesta, împreună cu DVD-ul, urmând să fie amplasate într-un spațiu securizat, cu acces limitat) și dezactivarea aplicației prin care se permite accesarea imaginilor de la distanță prin internet, prin stabilirea, în cadrul adunării generale a asociației de proprietari, a unui număr limitat de persoane care să aibă acces la acest sistem, al drepturilor ce pot fi alocate fiecăreia dintre acestea, al prevederii unor instrucțiuni clare de prelucrare pentru persoanele care prelucrează date sub autoritatea asociației, astfel încât să se evite accesarea, diseminarea sau prelucrarea în alt mod neautorizat a datelor personale prelucrate prin intermediul acestui sistem;

- asigurarea informării complete a persoanelor vizate, prin furnizarea tuturor informațiilor prevăzute de art. 12-13 din Regulamentul (UE) 2016/679, la loc vizibil, în apropierea camerelor de supraveghere instalate.

5. Investigații referitoare la prelucrarea datelor personale de către autorități publice

Instituțiile publice prelucrează un număr semnificativ de date cu caracter personal, de exemplu, în vederea aplicării legislației privind ocuparea forței de muncă, asistență și protecție socială, asigurări sociale, fiscalitate, în domeniul sănătății, educației, dar și date personale ale salariaților proprii sau chiar ale petenților care adresează diverse cereri către acestea.

Având în vedere faptul că instituțiile publice prelucrează cantități impresionante de date cu caracter personal, de cele mai multe ori din categoria celor speciale reglementate de Regulamentul (UE) 2016/679, acești operatori trebuie să se asigure că datele cu caracter personal sunt prelucrate cu respectarea principiilor stabilite de actul normativ european, într-un mod care asigură securitatea adecvată a datelor cu caracter personal, prin luarea de măsuri tehnice si organizatorice corespunzătoare.

În anul 2020, Autoritatea națională de supraveghere a înregistrat plângeri care au avut ca obiect o posibilă încălcare a legislației privind protecția datelor personale de către autorități publice.

FIȘĂ DE CAZ

O persoană fizică a reclamat faptul că o instituție publică i-a dezvăluit pe intranet-ul instituției date din dosarul său personal, inclusiv funcțiile ocupate, sancțiunile disciplinare, precum și calificativele anuale.

În cadrul investigației efectuate, s-a constatat că operatorul nu a adoptat suficiente măsuri tehnice și organizatorice în vederea asigurării confidențialității datelor prelucrate în legătură cu procedura de analizare a cererilor de mutare a patru persoane, printre care și petentul, de la o altă structură a autorității, prin postarea pe intranet-ul instituției a notelor-raport, inclusiv a notei-raport privindu-l pe petent, permițând astfel accesarea datelor personale ale acestor persoane de către angajați care nu aveau atribuții de serviciu în legătură cu soluționarea cererilor de mutare.

În acest caz s-a constatat încălcarea prevederilor art. 25 și 32 din Regulamentul (UE) 2016/679, dispunându-se sancționarea cu avertisment a operatorului.

De asemenea, au fost impuse prin planul de remediere o serie de măsuri ce vizau revizuirea procedurilor interne și instruirea personalului propriu, pentru a se evita situațiile de accesare sau divulgare neautorizată a datelor personale; în acest sens, s-a dispus inclusiv stabilirea responsabilităților și separarea rolurilor în accesarea informațiilor și documentelor postate pe rețeaua intranet utilizată în cadrul operatorului, în funcție de atribuțiile de serviciu.

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată cu privire la faptul că primăria unui municipiu a dezvăluit datele unor terți în cadrul unui litigiu dintre petent și aceasta, într-un dosar aflat pe rolul instanțelor judecătorești, în care primăria a solicitat înlocuirea amenzii aplicate petentului cu sancțiunea obligării la prestarea unei munci neremunerate în folosul comunității. În susținerea acțiunii, reclamantul a depus o serie de documente emise de primărie, în care figurau, pe lângă datele petentului, datele personale ale altor persoane (nume, prenume, cod numeric personal, adrese de domiciliu) care nu aveau calitate procesuală în respectivul dosar.

În cadrul investigației, operatorul a recunoscut faptul că, din eroare, la data sesizării instanței cu o acțiune formulată împotriva petentului, au fost depuse și alte documente care cuprind, pe lângă datele acestui contribuabil, datele de identificare ale altor persoane fizice, fără a se lua măsuri astfel încât să nu se dezvăluie datele acestora. În mod similar s-a procedat prin dezvăluirea datelor petentului în alte patru dosare de pe rolul instanței, vizând pe alți contribuabili.

În consecință, s-a dispus sancționarea cu avertisment a operatorului pentru încălcarea art. 32 din Regulamentul (UE) 2016/679, întrucât nu a prezentat dovezi din care să rezulte că a adoptat măsuri tehnice și organizatorice adecvate în vederea asigurării confidențialității datelor prelucrate în legătură cu administrarea mijloacelor de probă în cadrul unora dintre acțiunile introduse pe rolul instanțelor judecătorești, permițând astfel dezvăluirea ilegală a datelor personale ale altor persoane fizice (contribuabili) care nu aveau legătură cu dosarele respective.

De asemenea, prin planul de remediere, s-a stabilit în sarcina operatorului obligația de a-și revizui procedurile interne și de a efectua instruirea personalului propriu, pentru a se evita situațiile de dezvăluire ilegală a datelor personale.

FIȘĂ DE CAZ

Un petent a reclamat faptul că la nivelul comunei în care locuiește este instalat un sistem de supraveghere video de către primărie, care nu respectă prevederile Regulamentului (UE) 2016/679, inclusiv sub aspectul dreptului la informare, a asigurării măsurilor de securitate, a lipsei unui responsabil cu protecția datelor. De asemenea, petentul a menționat că dreptul său la viață privată este afectat, având în vedere că una dintre camere este instalată pe un stâlp aflat în colțul proprietății sale.

În urma investigației, a rezultat că imaginile înregistrate pot fi vizualizate în timp real pe monitorul din biroul primarului, dar și de la distanță, fără a exista precizări clare referitoare la măsurile de securitate implementate împotriva unor accesări ori divulgări ilegale ori accidentale.

De asemenea, nu au fost prezentate dovezi cu privire la realizarea unei informări complete a persoanelor vizate în legătură cu prelucrarea datelor lor, în legătură cu funcționarea sistemului de supraveghere video, în conformitate cu art. 12-13 din Regulamentul (UE) 2016/679.

Ca urmare a investigației efectuate, s-a constatat că operatorul a încălcat prevederile art. 12, 13, 32 și 37 alin. (1) și (7) din Regulamentul (UE) 2016/679, întrucât nu a prezentat dovezi din care să rezulte că a asigurat informarea corectă și completă a persoanelor vizate ale căror imagini sunt colectate prin intermediul sistemului de supraveghere video. De asemenea, nu a adoptat măsuri tehnice și organizatorice adecvate în vederea asigurării confidențialității datelor prelucrate (inclusiv în legătură cu autorizarea unui număr restrâns de persoane), conform atribuțiilor din fișa postului, de a avea acces limitat și securizat la imagini și la înregistrările provenite din sistemul de supraveghere video, numai în situația producerii unor incidente corespunzătoare scopului pentru care au fost instalate camerele. În același timp, s-a constatat că nu a desemnat un responsabil cu protecția datelor, conform obligațiilor ce îi reveneau conform art. 37 alin. (1) lit. a) din Regulamentul (UE) 2016/679, și nici nu a comunicat datele de contact

ale acestuia către Autoritatea națională de supraveghere și către public, așa cum prevede art. 37 alin. (7) din Regulamentul (UE) 2016/679.

Față de constatări, operatorul a fost sancționat cu avertisment și s-au dispus trei măsuri, prin planul de remediere, care se refereau:

- la informarea tuturor categoriilor de persoane vizate în legătură cu sistemul de supraveghere video,
- la adoptarea de măsuri tehnice și organizatorice adecvate cu privire la sistemul de supraveghere video, inclusiv cu privire la limitarea numărului de persoane autorizate potrivit fișelor de post care să aibă acces la imagini și înregistrări numai în situația producerii unor incidente care au legătură cu scopul instalării acestor camere de supraveghere, interzicerea accesului de la distanță prin internet la imagini și înregistrări, alocarea monitoarelor de urmărire a imaginilor în timp real numai în sarcina de vizualizare a persoanelor autorizate și
- la comunicarea către Autoritatea națională de supraveghere și către public a datelor de contact ale persoanei responsabile cu protecția datelor personale la nivelul operatorului.

De asemenea, s-a recomandat reanalizarea legalității instalării și a unghiului de orientare a camerelor de supraveghere video de către primărie, astfel încât să nu fie surprinse imagini de pe proprietățile private.

FIȘĂ DE CAZ

Autoritatea naţională de supraveghere a fost sesizată de către un petent cu privire la faptul că o autoritate publică nu a răspuns la cererile sale de exercitare a dreptului de acces.

În cadrul investigației s-a constatat că petentul a transmis operatorului cinci cereri, la un anumit interval de timp, prin care a solicitat și informații referitoare la datele sale personale și ale copiilor săi minori, prelucrate de către respectiva autoritate, la care avea înregistrată o cerere administrativă. Urmare a cererilor primite, operatorul a transmis petentului două răspunsuri. Astfel, primul răspuns transmis petentului nu conținea informații cu privire la dreptul de acces, iar în cel de-al doilea răspuns se invocau anumite prevederi din Legea nr. 677/2001, abrogată din 25 mai 2018.

Astfel, operatorul nu numai că nu a furnizat petentului informațiile solicitate, referitoare la data nașterii, locul nașterii, numele și prenumele părinților, copiii minori ai petentului, ci i-a furnizat și informații eronate referitoare la prevederi legale abrogate (Legea nr. 677/2001).

Ca urmare a investigației efectuate, s-a constatat că operatorul nu a respectat dispozițiile legale privind prelucrarea datelor cu caracter personal și a încălcat dispozițiiile art. 12 și art. 15 din Regulamentul (UE) 2016/679, întrucât nu a făcut dovada că a transmis petentului un răspuns la cererile prin care acesta și-a exercitat dreptul de acces.

Față de constatări, operatorul a fost sancționat contravențional și s-a dispus, ca măsură corectivă, să transmită un răspuns petentului la cererile prin care și-a exercitat dreptul de acces prevăzut de art. 15 din Regulamentul (UE) 2016/679.

FIȘĂ DE CAZ

Un petent a reclamat faptul că poliția locală din cadrul unei unități administrativ-teritoriale i-a dezvăluit datele cu caracter personal (nume, prenume, adresă, calitatea de proprietar al unui garaj), prin afișarea unui înscris (invitație) pe ușa garajului pe care îl deține, situat într-o zonă accesibilă publicului.

În urma investigației, s-a constatat că reprezentanți ai poliției locale au afișat pe garajul petentului o invitație de a se prezenta la sediul primăriei de pe raza teritorială în care acesta domiciliază, în vederea desfășurării unui control privind activitatea ”utilizare garaj”, întrucât petenții nu ar fi putut fi contactați direct, la domiciliu.

Astfel, prin afișarea respectivei invitații, s-a permis accesul unor terți la datele personale ale petentului, fără a se încerca o modalitate de transmitere a invitației care să asigure confidențialitatea datelor personale.

Față de constatări, s-a aplicat operatorului o sancțiune cu avertisment pentru încălcarea prevederilor art. 32 din Regulamentul (UE) 2016/679, sub aspectul capacității de a asigura confidențialitatea datelor și măsura corectivă de a revizui procedurile interne și de a instrui personalul propriu, pentru a se evita situațiile de dezvăluire a datelor personale.

6. Investigații referitoare la încălcarea principiilor și a legalității prelucrării datelor cu caracter personal

În multe dintre cazurile investigate de Autoritatea națională de supraveghere în anul 2020 în baza plângerilor primite, s-a urmărit respectarea principiilor prevăzute de Regulamentul (UE) 2016/679, precum și a condițiilor ce vizează asigurarea legalității prelucrărilor de date efectuate de diverși operatori.

Pentru situațiile în care s-a constatat, spre exemplu, prelucrarea datelor în scopuri incompatibile cu cele pentru care datele au fost colectate inițial ori a unor date care nu mai erau necesare pentru atingerea scopului propus sau efectuarea unor prelucrări de date fără să existe un temei legal adecvat, au fost aplicate sancțiuni împotriva operatorilor responsabili și s-a dispus remedierea deficiențelor identificate.

Prezentăm în continuare câteva cazuri relevante în acest sens:

FIȘĂ DE CAZ

Autoritatea națională de supraveghere a fost sesizată de către un petent cu privire la faptul că o instituție de credit i-a transmis mesaje privind actualizarea datelor sale cu caracter personal, deși relația sa contractuală cu această bancă era încheiată, ca urmare a cererii acestuia de închidere a contului curent deschis la această bancă. Ulterior, petentul a primit pe adresa sa de e-mail un nou mesaj referitor la actualizarea datelor sale cu caracter personal.

Din investigația efectuată, a reieșit că petentul și-a furnizat datele, respectiv adresa de e-mail, la deschiderea relației de afaceri cu banca, respectiv deschiderea unui cont curent. Ca urmare a unei erori de sistem, cererea de închidere a ultimului produs bancar deținut de client nu a avut ca efect și închiderea relației de afaceri, aceasta fiind păstrată în continuare cu status „activ". Ulterior, operatorul a transmis pe adresa de e-mail a petentului mai multe mesaje privind actualizarea datelor sale cu caracter personal, ca urmare a expirării cărții sale de identitate.

În vederea transmiterii celor trei mesaje au fost prelucrate mai multe date cu caracter personal, respectiv, adresa de e-mail, numele si prenumele, precum și data de expirare a cărtii de identitate.

Astfel, au fost încălcate prevederile art. 5 din Regulamentul (UE) 2016/679, care reglementează principiile legate de prelucrarea datelor cu caracter personal, conform cărora datele cu caracter personal (în speță, adresa de e-mail, numele și prenumele petentului, data de expirare a cărții de identitate) trebuie să fie:

a) prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată ("legalitate, echitate şi transparenţă");

b) colectate în scopuri determinate, explicite şi legitime şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri ("limitări legate de scop”);

c) adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate ("reducerea la minimum a datelor");

d) exacte şi, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere ("exactitate").

De asemenea, au fost încălcate prevederile art. 6 din Regulamentul (UE) 2016/679, întrucât, după încetarea relației de afaceri dintre operator și petent, operatorul nu mai avea temei legal pentru prelucrarea adresei de e-mail a petentului, coroborat cu numele și prenumele acestuia, data de expirare a cărții de identitate, în scopul transmiterii mesajelor.

Față de constatări, operatorul a fost sancționat contravențional cu amendă și i s-a recomandat să asigure conformitatea operațiunilor de prelucrare a datelor personale, în cadrul activităților desfășurate de bancă, cu principiile reglementate prin Regulamentul (UE) 2016/679 la art. 5, precum și cu prevederile art. 6 din același Regulament.

FIȘĂ DE CAZ

Un petent a reclamat faptul că o autoritate publică, angajator al petentului, a divulgat datele sale cu caracter personal, respectiv numele, prenumele, adresa și codul numeric personal, numărul de telefon, e-mail, sancțiuni disciplinare ale petentului, către un terț, respectiv unui alt angajat al operatorului de date.

Datele petentului au fost divulgate de operatorul de date către terț, prin înmânarea unor copii de pe documente care formează obiectul unui dosar aflat pe rolul unei instanțe

judecătorești, în care petentul și angajatorul sunt părți, terțul coleg neavând nicio calitate în respectivul proces.

Din investigația efectuată de Autoritatea națională de supraveghere, a reieșit că, deși terțul coleg avea cunoștință despre dosarul aflat pe rolul instanțelor de judecată, în care petentul era reclamant și autoritatea publică pârât, în virtutea atribuțiilor pe care le-a îndeplinit de-a lungul timpului în cadrul acestei autorități, pentru transmiterea documentelor din dosar către un terț în acel dosar, autoritatea publică, în calitate de operator, trebuia să respecte prevederile Regulamentului (UE) 2016/679, în special art. 5 și art. 6.

Or, aceasta nu a prezentat dovezi că transmiterea datelor cu caracter personal ale petentului, cuprinse în înscrisurile din dosar, înmânate în copie terțului coleg, a fost efectuată cu consimțământul petentului sau în baza altui temei legal reglementat la art. 6 din Regulamentul (UE) 2016/679.

De asemenea, prin transmiterea datelor cu caracter personal ale petentului, cuprinse în înscrisurile din dosar, prin înmânarea în copie a acestor înscrisuri terțului coleg, autoritatea publică a încălcat prevederile art. 5 din Regulamentul (UE) 2016/679 care reglementează principiile legate de prelucrarea datelor cu caracter personal, conform cărora datele personale (numele, prenumele, adresa și codul numeric personal, numărul de telefon, e-mail, sancțiuni disciplinare ale petentului) trebuie prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată și în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri .

Față de constatări, operatorul a fost sancționat contravențional și s-a dispus, în planul de remediere anexat la procesul-verbal, luarea unor măsuri, astfel încât datele personale ale angajaților cuprinse în înscrisurile din dosarele în care angajații operatorului au calitatea de reclamant sau pârât, să fie prelucrate cu respectarea prevederilor art. 5 alin. (1) lit. a) și b) și art. 6 din Regulamentul (UE) 2016/679.

FIȘĂ DE CAZ

Un petent a sesizat faptul că o persoană fizică a depus într-un proces aflat pe rolul instanțelor de judecată, în care petentul nu este parte, mai multe documente care conțin datele sale cu caracter personal, în posesia cărora persoana fizică se află ca urmare a

calității sale de administrator a unei societăți comerciale, care are ca obiect de activitate efectuarea de traduceri autorizate.

Din investigația efectuată de Autoritatea națională de supaveghere, a reieșit că în cadrul societății comerciale, ca urmare a solicitării petentului, au fost traduse o serie de documente aparținând petentului, care conțineau datele cu caracter personal ale acestuia, respectiv numele, prenumele, localitatea de domiciliu și județul.

În paralel, administratorul societății comerciale avea pe rolul instanțelor de judecată un litigiu civil cu o rudă a petentului, litigiu al cărui obiect nu avea nicio tangență cu activitatea prestată de societatea comercială către petent și față de care acesta este un terț.

Societatea comercială, în calitate de operator de date cu caracter personal raportat la prelucrările de date pe care le efectuează ca urmare a prestării unor servicii lingvistice autorizate, trebuie să respecte prevederile Regulamentului (UE) 2016/679, în special art. 5 și art. 6.

Or, această societate comercială nu a prezentat dovezi că dezvăluirea datelor cu caracter personal ale petentului în instanță a fost efectuată cu consimțământul acestuia sau în baza altui temei legal reglementat la art. 6 din Regulamentul (UE) 2016/679, precum art. 6 alin. (1) lit. f) din acest Regulament; astfel, în cazul în speță, nu au fost prezentate dovezi din care să rezulte prevalența interesului legitim al operatorului asupra intereselor sau drepturilor şi libertăţilor petentului, în calitate de persoană vizată.

De asemenea, operatorul a transmis datele cu caracter personal ale petentului, cuprinse în înscrisurile care formau obiectul traducerii, în instanță, cu încălcarea art. 5 alin. (1) lit. a) și b) din Regulamentul (UE) 2016/679, care prevede că datele cu caracter personal trebuie să fie prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată și colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri, coroborat cu art. 5 alin. (2) din Regulamentul (UE) 2016/679.

Față de constatări, operatorul a fost sancționat contravențional și s-a recomandat acestuia să ia măsurile care se impun, astfel încât datele cu caracter personal ale persoanelor vizate, pe care le colectează în vederea prestării serviciilor lingvistice, să fie prelucrate cu respectarea prevederilor art. 5 și 6 din Regulamentul (UE) 2016/679.

CAPITOLUL IV

ACTIVITĂŢI ÎN DOMENIUL RELAŢIILOR INTERNAŢIONALE

În anul 2020, activitatea de relații externe a Autorităţii naţionale de supraveghere a fost influențată de pandemia COVID-19. Astfel, evenimentele la nivel european au fost organizate în format videoconferință (on-line), Autoritatea națională de supraveghere participând la 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 includ:

- 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,
- Comitetul de Cooperare Europol.

Comitetul European pentru Protecția Datelor

În anul 2020, Comitetul European pentru Protecția Datelor a adoptat un aviz pe marginea proiectului de listă de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor, în conformitate cu art. 35 alin. (5) din Regulamentul (UE) 2016/679, 10 avize pe marginea proiectelor de decizii ale autorităților de supraveghere referitoare la regulile corporatiste obligatorii pentru operatori/persoane împuternicite de operatori, 11 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, 10 avize pe marginea proiectului de cerințe cu privire la aprobarea cerințelor de acreditare a unui organism de certificare în conformitate cu art. 43 alin. (3) din Regulamentul (UE) 2016/679, un aviz pe marginea clauzelor contractuale standard înaintate în temeiul art. 28 alin. (8) din Regulamentul (UE) 2016/679, o decizie obligatorie în temeiul art. 65 alin. (1) litera (a) 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:

- orientări privind art. 46 alin. (2) litera (a) și art. 46 alin. (3) litera (b) din Regulamentul (UE) 2016/679 pentru transferurile de date cu caracter personal între SEE și autoritățile și organismele publice din afara SEE – documentul urmărește să ofere îndrumări cu privire la aplicarea art. 46 alin. (2) litera a) și art. 46 alin. (3) litera b) din Regulamentul (UE) 2016/679 în ceea ce privește transferul de date cu caracter personal de la autorități sau organisme publice din SEE către organisme publice din țări terțe sau organizații internaționale, în absența unei decizii privind caracterul adecvat al nivelului de protecție. Organismele publice pot folosi astfel de mecanisme, dar, bineînțeles, au libertatea de a alege alte instrumente care oferă garanții corespunzătoare în conformitate cu art. 46 din Regulamentul (UE) 2016/679. Orientările sunt menite să ofere o indicație cu privire la așteptările Comitetului European pentru Protecția Datelor în legătură cu garanțiile necesare a fi implementate printr-un instrument obligatoriu din punct de vedere juridic. Acest document acoperă transferurile internaționale de date între organisme publice care au loc pentru diverse scopuri de cooperare administrativă care intră în sfera Regulamentului (UE) 2016/679;
- orientări privind prelucrarea datelor referitoare la sănătate în scopul cercetării științifice în contextul epidemiei COVID-19 – prin acest document s-a urmărit clarificarea aspectelor privind utilizarea datelor de sănătate, în special temeiul legal al prelucrării, utilizarea ulterioară a datelor în scop de cercetare științifică, inclusiv sub aspect transfrontalier, precum și asigurarea drepturilor persoanelor vizate;
- orientări privind utilizarea datelor de localizare și a instrumentelor de urmărire a contactelor în contextul epidemiei COVID-19 – documentul urmărește evidențierea condițiilor și principiilor de utilizare proporțională a datelor de localizare în scopul monitorizării răspândirii virusului, respectiv a instrumentelor de depistare pentru a anunța persoanele aflate în apropierea altor persoane depistate ca infectate. Cu acest prilej, Comitetul European pentru Protecția Datelor subliniază că utilizarea acestor date trebuie să se facă voluntar de fiecare persoană și să nu se ajungă la monitorizarea

deplasărilor persoanei respective, iar principiile necesității și proporționalității trebuie să fie respectate în stabilirea măsurilor din această perioadă;

- orientări privind consimțământul – documentul este o versiune ușor actualizată a orientărilor privind consimțământul adoptate de Grupul de lucru „Articolul 29" și care au fost aprobate de Comitetul European pentru Protecția Datelor. Actualizarea a fost realizată întrucât s-a constatat necesitatea de a oferi clarificări suplimentare în ceea ce privește valabilitatea consimțământului acordat de persoana vizată atunci când interacționează cu barierele de cookie-uri („cookies walls");
- orientări privind interacțiunea dintre Directiva privind serviciile de plată revizuită și Regulamentul (UE) 2016/679 – acest document urmărește să ofere îndrumări suplimentare cu privire la aspectele legate de protecția datelor în contextul PSD2, în special cu privire la relația dintre dispozițiile relevante din Regulamentul (UE) 2016/679 și Directiva privind serviciile de plată revizuită. Prezentele orientări pun accent în special pe prelucrarea datelor cu caracter personal de către furnizorii de servicii de informații despre cont (AISP) și furnizorii de servicii de inițiere a plății (PISP). Documentul abordează condițiile pentru acordarea accesului la informațiile contului de plată de către furnizorii de servicii de plată care deservesc contul (ASPSP) și pentru prelucrarea datelor cu caracter personal de către PISP și AISP, inclusiv cerințele și garanțiile în legătură cu prelucrarea datelor cu caracter pesronal de către PISP și AISP în alte scopuri decât scopurile inițiale pentru care au fost colectate datele, mai ales atunci când au fost colectate în contextul furnizării unui serviciu de informare cu privire la cont. Orientările abordează, de asemenea, diferitele noțiuni de consimțământ explicit în temeiul Regulamentului (UE) 2016/679 și Directivei 2015/2366/UE, prelucrarea categoriilor speciale de date de către PISP și AISP, aplicarea principalelor principii legate de prelucrarea datelor cu caracter personal stabilite de Regulamentul (UE) 2016/679, în special reducerea la minimum a datelor, transparența, responsabilitatea și integritatea și confidențialitatea;
- recomandările privind garanțiile esențiale europene pentru măsurile de supraveghere, prin raportare la activitatea de transfer – ca urmare a hotărârii în cauza Schrems II, s-a constatat necesitatea actualizării documentului privind garanțiile esențiale europene, elaborate inițial ca răspuns la hotărârea pronunțată în cauza Schrems I. Obiectivul garanțiilor esențiale europene actualizate este de a furniza

elemente care să permită să se examineze dacă măsurile de supraveghere care permit accesul autorităților publice dintr-o țară terță la date cu caracter personal, în calitate de agenții naționale de securitate sau de autorități de aplicare a legii, pot fi considerate sau nu o ingerință justificată. Garanțiile esențiale europene fac parte din evaluarea care trebuie efectuată pentru a stabili dacă o țară terță asigură un nivel de protecție în esență echivalent cu cel garantat în cadrul UE, dar nu urmăresc, în sine, să definească toate elementele care sunt necesare pentru a considera că o țară terță asigură un astfel de nivel de protecție în conformitate cu articolul 45 din Regulamentul (UE) 2016/679. Aspectele prezentate în acest document ar trebui considerate drept garanțiile esențiale care trebuie să se regăsească în țara terță atunci când se evaluează ingerința, pe care o implică măsurile de supraveghere ale unei țări terțe, în dreptul la viață privată și la protecția datelor, nu o listă de elemente care demonstrează că regimul juridic al unei țări terțe în ansamblu asigură un nivel de protecție în esență echivalent;

- declarație privind prelucrarea datelor cu caracter personal în contextul epidemiei de COVID-19 – prin această declarație Comitetul European pentru Protecția Datelor subliniază faptul că, inclusiv în aceste momente excepționale, operatorul de date și persoana împuternicită de operator trebuie să asigure protecția datelor cu caracter personal ale persoanelor vizate. Astfel, documentul abordează aspecte privind legalitatea prelucrării, principiile de bază referitoare la prelucrarea datelor cu caracter personal, utilizarea datelor de localizare mobile, ocuparea forței de muncă;
- declarație privind restricțiile asupra drepturilor persoanelor vizate în contextul stării de urgență din statele membre – ca urmare a informării primite cu privire la adoptarea de către guvernul unui stat membru UE a unui decret privind derogările de la anumite dispoziții privind protecția datelor și accesul la informații pe durata stării de pericol, Comitetul European pentru Protecția Datelor a reamintit faptul că protecția datelor cu caracter personal nu împiedică lupta împotriva pandemiei de COVID-19 și că Regulamentul (UE) 2016/679 se aplică în continuare și permite luarea unor măsuri eficiente de răspuns în fața pandemiei, protejând totodată drepturile și libertățile fundamentale. De asemenea, declarația face vorbire de faptul că protecția datelor cu caracter personal trebuie respectată chiar și în această perioadă excepțională în cadrul tuturor măsurilor de urgență, inclusiv al restricțiilor adoptate la nivel național, iar orice

restricție trebuie să respecte esența dreptului care este restricționat. Totodată, Comitetul european pentru protecția datelor atrage atenția asupra faptului că restricțiile prevăzute trebuie să îndeplinească efectiv un obiectiv important de interes public general al Uniunii sau al unui stat membru a cărui realizare trebuie asigurată, așa cum este obiectivul sănătății publice în cazul stării de urgență actuale din unele state membre. În plus, se evidențiază faptul că, în conformitate cu jurisprudența Curții de Justiție a Uniunii Europene, toate restricțiile asupra drepturilor persoanelor vizate trebuie să se aplice numai în măsura în care acest lucru este strict necesar și proporțional în vederea îndeplinirii unui astfel de obiectiv de sănătate publică;

- declarație privind impactul pe care interoperabilitatea aplicațiilor de urmărire a contactelor îl are asupra protecției datelor – prin acest document, Comitetul European pentru Protecția Datelor reamintește faptul că utilizarea aplicațiilor de urmărire a contactelor se bazează pe prelucrarea de date cu caracter personal pseudonimizate ale utilizatorilor aplicațiilor. De asemenea, Comitetul este de părere că permiterea schimbului de date despre persoane care au fost diagnosticate sau testate pozitiv cu astfel de aplicații interoperabile trebuie declanșată numai printr-o acțiune voluntară a utilizatorului și că persoanele vizate trebuie să dețină controlul asupra propriilor date. Totodată, se evidențiază faptul că scopul interoperabilității nu trebuie utilizat ca argument pentru extinderea culegerii de date cu caracter personal mai mult decât este necesar. Aplicațiile de urmărire a contactelor pot reprezenta doar o soluție temporară, ca parte a unei strategii cuprinzătoare de sănătate publică pentru combaterea pandemiei actuale. Pentru fiecare măsură introdusă, trebuie să se evalueze dacă o alternativă mai puțin invazivă poate atinge același scop și să se asigure că măsurile aplicate sunt eficace și proporționale;

- întrebări frecvente cu privire la hotărârea Curții de Justiție a Uniunii Europene în cauza C-311/18 - Data Protection Commissioner împotriva Facebook Ireland Ltd și Maximillian Schrems – ca urmare a hotărârii CJUE în cauza C-113/18, Comitetul European pentru Protecția Datelor a adoptat documentul „Întrebări Frecvente” pentru a oferi clarificări inițiale și îndrumări preliminare părților interesate cu privire la folosirea instrumentelor legale pentru transferul de date cu caracter personal în state terțe, inclusiv în SUA. De reținut faptul că acest document va fi completat cu îndrumări

suplimentare, întrucât Comitetul va continua să examineze și să evalueze hotărârea CJUE;

- <u>notă de informare privind regulile corporatiste obligatorii (BCR) pentru grupurile de întreprinderi/societăți a căror autoritate de supraveghere principală pentru BCR este Oficiul Comisarului pentru Informații (ICO)</u> – documentul abordează două scenarii: 1) BCR autorizate și 2) cereri de BCR înaintate către ICO. În ambele scenarii, autoritatea de supraveghere din SEE care poate fi abordată pentru a acționa ca nouă autoritate de supraveghere principală pentru BCR va analiza, de la caz la caz, în baza criteriilor prevăzute în WP 263 și în colaborare cu alte autorități de supraveghere în cauză, dacă este autoritatea de supraveghere principală corespunzătoare pentru BCR și va informa grupul în consecință;
- <u>declarație referitoare la Regulamentul privind viața privată și comunicațiile electronice și viitorul rol al autorităților de supraveghere și al Comitetului european pentru protecția datelor</u> – prin declarația sa, Comitetul european pentru protecția datelor invită statele membre să sprijine un Regulament privind viața privată și comunicațiile electronice mai eficace și mai coerent, astfel cum a fost propus inițial de Comisia Europeană și astfel cum a fost modificat de Parlamentul European;
- <u>notă de informare privind transferul de date în temeiul Regulamentului (UE) 2016/679 către Regatul Unit după perioada de tranziție</u> – perioada de tranziție pentru retragerea Regatului Unit din Uniunea Europeană se va încheia la 31 decembrie 2020 ceea ce înseamnă că, începând cu 1 ianuarie 2021, Regatul Unit nu va mai aplica Regulamentul (UE) 2016/679 pentru prelucrarea datelor cu caracter personal. Prin urmare, începând cu data de 1 ianuarie 2021, toate transferurile de date cu caracter personal către Regatul Unit vor constitui transfer de date către o țară terță și, în consecință, va fi supus dispozițiilor capitolului V din Regulamentul (UE) 2016/679;
- <u>declarație referitorea la protecția datelor cu caracter personal prelucrate în contextul prevenirii spălării banilor și finanțării terorismului</u> – Comitetul European pentru Protecția Datelor consideră că este extrem de important ca măsurile de combatere a spălării banilor să fie compatibile cu dreptul la viață privată și dreptul la protecția datelor consacrate în art. 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene, cu principiile necesității unor astfel de măsuri într-o societate democratică și al

proporționalității acestora, precum și cu jurisprudența Curții de Justiție a Uniunii Europene.

În același timp, Comitetul European pentru Protecția Datelor a adoptat următoarele ghiduri și recomandări disponibile spre consultare publică și trimitere de propuneri:

- orientări privind privind prelucrarea datelor cu caracter personal în contextul vehiculelor conectate și al aplicațiilor legate de mobilitate;
- orientări privind conceptele de operator și persoană împuternicită de operator din Regulamentul (UE) 2016/679;
- orientări privind privind evidențierea utilizatorilor în mediile sociale;
- orientări privind conceptul de obiecție relevantă și motivată din perspectiva Regulamentului (UE) 2016/679;
- orientări privind restricțiile potrivit art. 23 din Regulamentul (UE) 2016/679;
- recomandările privind măsurile care suplimentează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a datelor cu caracter personal, ca urmare a Deciziei Curții de Justiție a Uniunii Europene în Cauza Schrems.

Comitetul Consultativ al Convenţiei 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.

Astfel, ca urmare a aprobării în luna februarie a anului 2020 a Memorandumului cu tema „Aprobarea semnării Protocolului de amendare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal”, coinițiat de Ministerul Afacerilor Externe împreună cu Autoritatea națională de supraveghere, prin

care s-a propus aprobarea semnării Protocolului de amendare a Convenției Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, Protocolul de amendare a Convenției 108 a fost semnat de România la data de 26 iunie 2020.

În anul 2020, Protocolul de amendare a Convenției 108 a fost semnat de Bosnia și Herțegovina și de Malta în data de 2 iulie 2020, iar de Liechtenstein în data de 7 decembrie 2020. De asemenea, tot în anul 2020 următoarele state au ratificat Convenția 108 modernizată acestea transmițând instrumentul de ratificare după cum urmează: Lituania în data de 23 ianuarie 2020, Serbia în data de 26 mai 2020, Polonia în data de 10 iunie 2020, Republica Maurițius în data de 4 septembrie 2020, Estonia în data de 16 septembrie 2020, Cipru în data de 21 septembrie 2020, Malta în data de 2 noiembrie 2020 și Finlanda în data de 10 decembrie 2020.

Comitetul de Cooperare Europol

În anul 2016, Organismul Comun Europol a emis un ghid pentru Unitățile naționale Europol intitulat „Manualul ENU". Având în vedere faptul că respectivul document a fost redactat în temeiul Deciziei Consiliului 2009/371/JAI, Comitetul de Cooperare Europol a decis actualizarea acestuia în conformitate cu Regulamentul (UE) 2016/794 (Regulamentul Europol).

Ajustările și modificările aduse Manualului se referă, spre exemplu, la sarcinile Unităților naționale Europol, responsabilitatea în materie de protecție a datelor, securitatea prelucrării datelor, evaluarea fiabilității sursei și a exactității informațiilor.

În același timp, Comitetul de Cooperare Europol a considerat că aceasta ar putea fi o bună oportunitate de a alinia manualul la nevoile și preocupările Unităților naționale Europol în ceea ce privește protecția datelor cu caracter personal. Ca atare, s-a decis lansarea unui sondaj pentru Unitățile naționale Europol care conține 3 părți: prima partea vizează identificarea cadrului juridic și practic în care operează Unitatea națională Europol, precum și relația dintre aceasta și autoritățile naționale competente; a doua parte evaluează gradul de satisfacție a Unității naționale Europol cu privire la orientările disponibile în prezent (indiferent dacă sunt furnizate de Europol, Organismul de Control Comun anterior sau de statul membru); iar a treia parte conține câteva aspecte pe

marginea cărora se dorește o contribuție specială, spre exemplu dreptul de acces, datele minorilor, competența Europol.

În ceea ce privește activitatea de promovare și facilitarea exercitării drepturilor persoanelor vizate, varianta finală a ghidului privind exercitarea drepturilor de către persoanele vizate în legătură cu sistemele de informații deținute de Europol, pentru care Autoritatea națională de supraveghere a fost raportor, a fost adoptată. Documentul oferă informații privind drepturile de care beneficiază persoanele vizate în temeiul Regulamentului Europol, categoriile de date care fac obiectul schimbului de informații între statele membre și Europol, precum și o descriere a procedurii pentru exercitarea dreptului de acces din fiecare stat membru, împreună cu datele de contact ale autorităților de supraveghere la care poate fi depusă o plângere.

Reguli Corporatiste Obligatorii

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

Regulile corporatiste obligatorii (BCRs) au fost introduse ca răspuns la nevoia organizațiilor de a avea o abordare globală în ceea ce privește protecția datelor cu caracter personal, în situația în care multe organizații dețineau mai multe filiale/sucursale situate pe tot globul, transferând date cu caracter personal la scară largă. Includerea BCRs în Regulamentul (UE) 2016/679 consolidează în continuare utilizarea lor ca garanție adecvată pentru a legitima transferurile de date cu caracter personal în țări terțe.

În anul 2020, Autoritatea națională de supraveghere a primit și a analizat cereri de aprobare a BCRs transmise de 69 de companii multinaționale. De asemenea, Autoritatea națională de supraveghere a acționat în calitate de autoritate principală pentru un set 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 2 companii în această perioadă și ca membru în echipa de redactare a două 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 recomandări dintre care evidențiem următoarele:

- precizarea în formularele standard WP264 (operator), respectiv WP265 (persoană împuternicită de operator) a motivelor pentru care Autoritatea națională de supraveghere a fost desemnată autoritate principală în legătură cu setul de reguli corporatiste obligatorii;
- introducerea unui nou paragraf prin care să se specifice faptul că responsabilul cu protecția datelor va păstra o evidență a cererilor primite de la persoanele vizate;
- introducerea unui paragraf prin care să se specifice faptul că toate plângerile primite de alți membri ai grupului vor fi imediat redirecționate către responsabilul cu protecția datelor;
- introducerea unui paragraf prin care să se specifice faptul că responsabilul cu protecția datelor va păstra o evidență a plângerilor primite de la persoanele vizate; de asemenea, în respectivul paragraf se poate menționa faptul că, în funcție de plângerile primite/necesitate, responsabilul cu protecția datelor va revizui prezenta procedură pentru soluționarea plângerilor;
- reformularea textului pentru a se asigura că auditul va aborda toate aspectele ce țin de regulile corporatiste obligatorii ale grupului, inclusiv toate sistemele IT relevante, bazele de date, politicile de securitate și, dacă este aplicabil, sistemele fizice de evidență ale grupului.

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 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 2020, Comitetul European pentru Protecția Datelor a emis 9 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 **56 solicitări** cu privire la aplicarea și respectarea Regulamentului (UE) 2016/679. Solicitările venite din partea autorităților de supraveghere din Cipru, Danemarca, Estonia, Germania, Italia, Letonia, Lituania, Luxemburg, Malta, Norvegia, Olanda, Polonia, Slovacia, Slovenia, Suedia, Ungaria au vizat aspecte referitoare la procedura de soluționare a plângerilor, interesul legitim ca temei legal pentru prelucrarea datelor cu caracter personal efectuată de autorități publice, aplicabilitatea Regulamentului (UE) 2016/679 în ceea ce privește prelucrarea în scop exclusiv personal, monitorizarea operațiunilor de prelucrare efectuate de instanțele care acționează în exercițiul funcției lor judiciare.

Contribuții pe marginea documentelor din perspectiva protecției datelor cu caracter personal

În cursul anului 2020, Autoritatea națională de supraveghere a formulat observații și propuneri pe marginea documentelor transmise de alte autorități/instituții:

- raportul anual 2019 și planul de lucru 2021 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;
- interoperabilitatea sistemelor de informații de la nivelul UE – Autoritatea națională de supraveghere a transmis o serie de observații pe marginea formularului standard prin care persoana va fi informată despre crearea unei conexiuni roșii/albe și a informării pentru cetățean, sub forma unei scrisori;
- completarea variantei revizuite a Chestionarului Schengen, astfel încât să se realizeze o actualizare a informațiilor deținute pentru a avea o imagine de ansamblu cât mai aproape de realitate;
- completarea chestionarului privind legislația națională în domeniul comerțului electronic elaborat de Secretariatul Conferinței Națiunilor Unite pentru Comerț și Dezvoltare (UNCTAD) – Autoritatea națională de supraveghere a transmis contribuția sa pe marginea secțiunii referitoare la protecția datelor cu caracter personal din cadrul

chestionarului în legătură cu adoptarea sau modificarea legislației naționale privind protecția datelor și a vieții private;

- proiectul de Memorandum Explicativ și propunerea Comisiei Europene de acord de prelucrare a datelor cu caracter personal de către operatorii asociați – Autoritatea națională de supraveghere a transmis o serie de observații pe marginea documentelor înaintate referitoare la principiile legate de prelucrarea datelor cu caracter personal, cu precădere principiul „limitării legate de stocare", drepturile persoanelor vizate și restricțiile prevăzute la art. 23 din Regulamentul (UE) 2016/679;
- elemente de mesaj ca urmare a hotărârii CJUE în cauza C-311/18 (Schrems II) – prin hotărârea din data de 16 iulie 2020 pronunțată în cauza C-113/18, Curtea de Justiție a Uniunii Europene a invalidat Decizia de punere în aplicare (UE) 2016/1250 a Comisiei din 12 iulie 2016 în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului privind caracterul adecvat al protecției oferite de Scutul de confidențialitate UE-SUA. Totodată, trebuie avut în vedere faptul că CJUE a examinat și validitatea Deciziei 2010/87/CE a Comisiei Europene privind clauzele contractuale standard și a considerat că este validă. Așa cum se menționează și în Hotarărea Curții, validitatea Deciziei 2010/87/CE nu este pusă în discuție prin simplul fapt că, având în vedere natura contractuală a acestor clauze, clauzele standard de protecție a datelor din respectiva decizie nu impun obligații autorităților din țările terțe în care pot fi transferate datele. Totuși, validitatea Deciziei 2010/87/CE depinde de faptul dacă această decizie include mecanisme eficiente care fac posibilă, în practică, asigurarea respectării nivelului de protecție în esență echivalent cu cel garantat de Regulamentul (UE) 2016/679 în UE și, în situația în care aceste clauze sunt încălcate sau respectarea acestora este imposibilă, transferurile de date în temeiul acestor clauze sunt suspendate sau interzise. Din acest punct de vedere, s-a evidențiat faptul că Decizia din 2010/87/CE impune obligația unui exportator de date și a destinatarului („importatorul de date") de a verifica, înainte de orice transfer și, ținând seama de circumstanțele transferului, dacă acest nivel de protecție este respectat în țara terță și că Decizia din 2010/87/CE impune importatorului de date să informeze exportatorul de date cu privire la orice incapacitate de a respecta clauzele standard de protecție a datelor și, dacă este necesar, orice măsuri suplimentare celor oferite de clauza respectivă, acesta din urmă fiind, la rândul său, obligat să

suspende transferul de date și/sau să rezilieze contractul cu primul. Realizarea unui transfer de date în temeiul clauzelor contractuale standard depinde de rezultatul evaluării efectuate de exportatorul de date, luând în considerare circumstanțele transferurilor și de măsurile suplimentare pe care exportatorul de date le-ar putea implementa. Măsurile suplimentare, împreună cu clauzele contractuale standard, în urma unei analize de la caz la caz a circumstanțelor din jurul transferului, ar trebui să se asigure că legislația SUA nu afectează nivelul adecvat de protecție pe care îl garantează. În acest context, Curtea a subliniat că este responsabilitatea principală a exportatorului de date și a importatorului de date să realizeze această evaluare și să prevadă măsurile suplimentare necesare. Referitor la Decizia Comisiei Europene (UE) 2016/1250, CJUE a examinat validitatea acestei Decizii prin prisma cerințelor derivate din Regulamentul (UE) 2016/679, ținând cont de dispozițiile Cartei care garantează respectarea vieții private și de familie, protecția datelor cu caracter personal și dreptul la o protecție judiciară eficientă. În opinia CJUE, limitele privind protecția datelor cu caracter personal care decurg din dreptul intern al Statelor Unite privind accesul și utilizarea de către autoritățile publice americane a acestor date transferate din Uniunea Europeană în țara terță nu sunt circumscrise într-un mod care să satisfacă cerințe care sunt în mod esențial echivalente cu cele impuse de legislația Uniunii Europene, prin principiul proporționalității, în măsura în care programele de supraveghere bazate pe aceste dispoziții nu se limitează la ceea ce este strict necesar. Totodată, CJUE a subliniat faptul că, deși aceste dispoziții stabilesc cerințele pe care autoritățile americane trebuie să le respecte în momentul punerii în aplicare a programelor de supraveghere în cauză, dispozițiile nu acordă persoanelor vizate drepturi acționabile în fața instanțelor împotriva autorităților americane. În ceea ce privește cerința protecției judiciare, în opinia CJUE, mecanismul Ombudsmanului pentru Scutul de confidențialitate nu oferă garanții echivalente cu cele impuse de legislația UE, astfel încât să se asigure independența Ombudsmanului prevăzut de acest mecanism. În acest sens, CJUE a reținut că decizia menționată nu conține nicio indicație potrivit căreia acest Ombudsman ar fi abilitat să adopte decizii obligatorii în privința respectivelor servicii și nici nu menționează garanțiile legale care ar însoți acest angajament și de care s-ar putea prevala persoanele vizate astfel că, în consecință, mecanismul de tip Ombudsman prevăzut de Decizia Comisiei Europene (UE) 2016/1250 nu furnizează o cale

de atac în fața unui organ care oferă persoanelor ale căror date sunt transferate către Statele Unite garanții în esență echivalente cu cele prevăzute la articolul 47 din Carta drepturilor fundamentale a Uniunii Europene. 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 Statele Unite poate fi efectuat în conformitate cu unul din următoarele instrumente prevăzute de art. 46 din Regulamentul (UE) 2016/679: i) clauze standard de protecție a datelor, ii) reguli corporatiste obligatorii, iii) 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 Statele Unite ale Americii 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. 5/2020 a bugetului de stat pe anul 2020 un buget inițial în sumă de 6.219.000 lei, modificat în conformitate cu prevederile Ordonanţelor de Urgență ale Guvernului nr. 50/2020, nr. 135/2020 și nr. 201/2020.

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

Comparație buget anual 2016-2020

Anul	2016	2017	2018	2019	2020
Buget final (mii lei)	4.851	4.287	4.735	5.147	4.903
% față de anul anterior		88,37%	110,45%	108,70 %	95,26 %

Bugetul anului 2020 a fost mai mic cu aproximativ 5% față de bugetul anului anterior.

Dat fiind că modul de concepere a bugetelor pune un accent semnificativ pe sumele cheltuite anterior, din cauza numărului mic de personal și a faptului că sumele necesare depășesc semnificativ alocările anterioare la capitolul investiții, bugetele aprobate pentru Autoritatea națională de supraveghere au rămas la un nivel care asigură funcționarea nu și dezvoltarea.

Comparativ cu alte instituții similare din UE, bugetul autorității a fost în mod constant mai mic decât al autorității de supraveghere din Bulgaria, iar în ultimii 2 ani mai mic și față de cel al autorității similare din Croația. Bugete mai mici (echivalent in euro) decât cel al Autorității naționale de supraveghere au avut în ultimii ani doar Cipru, Malta, Estonia și Letonia, țări cu o populație semnificativ mai mică decât România.

Având în vedere aceste aspecte și în urma anulărilor de credite realizate în luna decembrie 2020, conform reglementărilor Legii nr. 500/2002 privind finanţele publice, rezultă următoarea sinteză:

Denumire indicator	Cod	Buget iniţial 2020 - mii lei -	Buget actualizat la 31.12.2020 - mii lei -	Execuție bugetară la 31.12.2020 - mii lei -	Execuţie bugetară la 31.12.2020 (%)
Total cheltuieli	51.01	6.219	4.903	4.809	98,08
Titlul I Cheltuieli de personal	10	5.239	3.973	3.956	99,58
Titlul II Bunuri şi servicii	20	880	830	757	91,24
Cheltuieli de capital Titlul XIII Active nefinanciare	71	100	100	95	95,44

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

Un impact semnificativ asupra bugetului Autorității naționale de supraveghere și asupra execuției bugetare a avut pandemia Covid-19, pe parcursul anului 2020 fiind interzisă organizarea concursurilor pentru ocuparea posturilor vacante. De asemenea, nu au putut fi realizate deplasări, iar unele achiziții preconizate nu s-au putut realiza datorită modificărilor din piața de bunuri și servicii generate de pandemie.

În acest context, creditele definitive aprobate au asigurat continuitatea activității Autorității naționale de supraveghere, ținându-se cont de măsurile luate în scopul prevenirii răspândirii infectării cu coronavirus și de eficiența utilizării fondurilor publice.

În ceea ce priveşte modul de repartizare a fondurilor alocate, putem preciza că suma aferentă cheltuielilor de personal ale Autorităţii naționale de supraveghere a constituit un procent de 81,03% din totalul creditelor repartizate de la bugetul de stat, din care s-au utilizat efectiv credite în valoare de 3.956.198 lei (datorită vacantării unor posturi prin pensionare, demisii sau încetarea unor detașări), înregistrându-se 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 – inclusiv demnitarii – din totalul de 87 posturi).

Majoritatea cheltuielilor de personal au fost aferente plăţilor efectuate pentru munca salariată a angajaţilor din compartimentele de specialitate.

Cheltuielile aferente titlului Bunuri și servicii în anul 2020 au avut o pondere de 16,92% în bugetul instituției, iar din acestea, cheltuielile cu pondere mai importantă au fost:

I. 41% costuri de închiriere și cheltuieli 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, abonament program legislativ, furnituri de birou și alte materiale necesare desfășurării activității etc.). De menționat și cheltuielile generate de pandemie, neprevăzute și nebugetate, în sumă totală de 24.902 lei și care au reprezentat 3,28% din totalul plăților aferente în anul 2020 cheltuielilor cu bunuri și servicii.

În anul 2020, cheltuielile cu bunuri și servicii au scăzut cu 9 % față de anul 2019, în contextul pandemiei de coronavirus.

De asemenea, trebuie precizat faptul că s-au avut permanent în vedere factori precum: oportunitatea cheltuielilor, criteriul prețului celui mai scăzut aplicat în procedurile de achiziții publice, alăturat unor cerinţe tehnice atent stabilite – ceea ce a condus la utilizarea eficientă a fondurilor bugetare alocate la Titlul II Bunuri și servicii.

În ceea ce privește Titlul X Active nefinanciare, în anul 2020, Autoritatea naţională de supraveghere a continuat – în măsura posibilităților oferite de alocările bugetare – proiectul de reînnoire a infrastructurii IT, în acest scop fiind utilizate fondurile prevăzute în bugetul final al titlului Cheltuieli de capital. Acest proiect a fost 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.

Politicile contabile utilizate la întocmirea situaţiilor financiare anuale sunt în conformitate cu reglementările legale în vigoare.

Situaţiile financiare anuale oferă o imagine fidelă a realităţii poziţiei financiare a Autorității naţionale de supraveghere și informații privind încadrarea în creditele bugetare alocate pe grupe, titluri, articole şi alineate de cheltuieli, aşa cum sunt prevăzute acestea în bugetul autorităţii.

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 şi printr-o atentă administrare de către Autoritatea națională de supraveghere.